日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２９日

出願番号
Application Number: 特願２００３－０２０９３７

[ST. 10/C]: [ＪＰ２００３－０２０９３７]

出願人
Applicant(s): シャープ株式会社

２００３年１２月２４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１０６９５１

【書類名】　特許願
【整理番号】　02J03829
【提出日】　平成15年 1月29日
【あて先】　特許庁長官　殿
【国際特許分類】　B41J 29/38
G03G 21/00
G06F 3/12
G06F 15/16
【発明者】
【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
【氏名】　朝田　直樹
【発明者】
【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
【氏名】　山下　博
【特許出願人】
【識別番号】　000005049
【氏名又は名称】　シャープ株式会社
【代理人】
【識別番号】　100080034
【弁理士】
【氏名又は名称】　原　謙三
【電話番号】　06-6351-4384
【選任した代理人】
【識別番号】　100113701
【弁理士】
【氏名又は名称】　木島　隆一

【選任した代理人】

【識別番号】　100116241

【弁理士】

【氏名又は名称】　金子　一郎

【手数料の表示】

【予納台帳番号】　003229

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0208489

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法

【特許請求の範囲】

【請求項１】

ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおいて、

上記電子機器、記憶手段および外部機器は、それぞれがセキュリティ機能を有していることを特徴とする電子機器ネットワークシステム。

【請求項２】

上記電子機器、記憶手段および外部機器が有しているセキュリティ機能のセキュリティレベルに応じて、上記電子機器、記憶手段および外部機器を検索する検索手段を備えていることを特徴とする請求項１に記載の電子機器ネットワークシステム。

【請求項３】

上記外部機器の設置場所または外部機器が備えている機能に基づいて、上記外部機器の検索を行う検索手段を備えていることを特徴とする請求項１または２に記載の電子機器ネットワークシステム。

【請求項４】

上記検索手段は、上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することを特徴とする請求項２または３に記載の電子機器ネットワークシステム。

【請求項５】

上記外部機器は、自機のセキュリティレベルに対応する記憶手段を検索する検索部を備えていることを特徴とする請求項１～４の何れか１項に記載の電子機器ネットワークシステム。

【請求項６】

上記電子機器は、上記検索手段による検索条件を入力し、該検索結果を表示する表示手段を備えていることを特徴とする請求項１～５の何れか１項に記載の電子機器ネットワークシステム。

【請求項７】

上記電子機器、記憶手段および外部機器のセキュリティ機能は、アクセス制御手段を介して接続された複数のネットワークのうち、どのネットワークに配置されているかによって付与されることを特徴とする請求項１～６の何れか１項に記載の電子機器ネットワークシステム。

【請求項８】

上記外部機器は、画像形成装置であることを特徴とする請求項１～７の何れか１項に記載の電子機器ネットワークシステム。

【請求項９】

上記電子機器は、スキャナ装置であることを特徴とする請求項１～８の何れか１項に記載の電子機器ネットワークシステム。

【請求項１０】

ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおけるデータ送信方法において、

上記電子機器、記憶手段および外部機器は、それぞれセキュリティ機能を有しており、

上記電子機器からデータを送信する場合には、ユーザが設定したセキュリティレベルに応じて、該セキュリティレベルに適合するセキュリティ機能を備えた上記記憶手段および外部機器の検索を行うことを特徴とする電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項１１】

上記外部機器の検索は、外部機器の設置場所、機能に基づいて行われることを特徴とする請求項１０に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項１２】

上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することを特徴とする請求項１０または１１に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項１３】

セキュリティレベルが合致しない上記電子機器、上記記憶手段および上記外部機器に対するデータの送信を禁止することを特徴とする請求項１０～１２の何れか１項に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【請求項１４】

上記外部機器から上記記憶手段に格納されたデータを取り出す際に、必要なデータが格納されている記憶手段とセキュリティレベルが合致せずに該外部機器に対してデータを送信できない場合には、

上記検索手段が、上記必要なデータが格納されている記憶手段とセキュリティレベルが適合する外部機器を検索することを特徴とする請求項１３に記載の電子機器ネットワークシステムによるデータ送信先検索方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数の電子機器がネットワークを介して接続されて構成されており、各電子機器から送信されるデータに基づいて、他の電子機器において出力する電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法に関するものである。

【０００２】

【従来の技術】

情報処理機器の発展およびインターネット環境の急速な充実に伴い、旧来のＬＡＮ環境で用いられている技術に加え、インターネットで利用される様々な技術を適用したＯＡ機器が開発されている。

【０００３】

このようなＯＡ機器を使用すれば、各々の機器の個別利用にとどまらず、複数

の機能を組み合わせて利用することも可能になる。また、このようなＯＡ機器は、コンピュータ機器の外部装置として利用されるだけではなく、逆にコンピュータ機器を外部装置として利用することも可能である。すなわち、ＯＡ機器は高度情報処理機器としての側面を備えており、オフィスにおける知的生産作業を支援するサービスを提供する機器となりつつある。

【０００４】

このような情報処理機器の発展に伴い、１９９８年５月に設立されたＯＡシステム機器プロジェクト委員会は、ＯＡ機器の新たな統合インターフェース仕様としてBMLinkSを開発した。

【０００５】

このBMLinkSの規格として、ホストコンピュータ（ホストＰＣ）から送信した印刷データをストレージサーバに格納し、この格納した印刷データをストレージサーバからプリンタに送信して印刷出力する印刷システムがある。

【０００６】

また、ネットワーク上に情報処理装置やプリンタ等が分散配置された印刷システムにおいて、印刷データを出力するためのプリンタを検索して、検索されたプリンタに印刷データを送信し、出力させるといったプリントシステムがある（特許文献１参照）。

【０００７】

特許文献１では、ユーザが作成した印刷ジョブに適した機能（用紙サイズ、両面印刷、ソート等）やフォーマット（ビットマップ、プリンタ言語等）を検索し、出力するプリントシステムが提案されている。

【０００８】

ネットワークやインターネットが急速に発展している昨今、上述のような印刷システムは非常に便利なものであり、利用価値が高い。

【０００９】

しかし、上記特許文献１に開示されたプリントシステムは、印刷データの保護（セキュリティ）という観点に立って構築されていない。このため、機密文書などを印刷する場合に、データ漏洩などの危険性があり、安易に利用することがで

きない。

【００１０】

そこで、印刷データのパスワードを付加し、そのパスワードを入力して印刷出力や印刷データの削除を可能にすることで、印刷データの漏洩等の問題を解決した印刷システムがある（特許文献２・３参照）。

【００１１】

例えば、特許文献２に開示されたデータ出力制御システムでは、セキュリティ印刷モードに設定されると、プリントサーバにおいて、ＩＤおよびパスワードが照合されない限り、印刷データをプリント装置へ出力しないように制御することで、データ漏洩等の問題を解決している。

【００１２】

【特許文献１】

特開平０７－２１４８７２号公報（公開日１９９５年８月１５日）

【００１３】

【特許文献２】

特開平１０－０２１０２２号公報（公開日１９９８年１月２３日）

【００１４】

【特許文献３】

特開平１１－３０１０５８号公報（公開日１９９９年１１月２日）

【００１５】

【発明が解決しようとする課題】

しかしながら、上記特許文献２に開示されたシステムでは、ＩＤおよびパスワードの入力により安全性を確保しているが、ＩＤおよびパスワードが分からないユーザにはセキュリティ印刷モードでプリンタの利用ができないという問題を有している。

【００１６】

本発明は、上記の問題点に鑑みてなされたものであり、その目的は、ネットワークを構成する電子機器間において送信されるデータの保護（セキュリティ）を考慮しつつ、ユーザが自由にセキュリティレベルに応じた送信ルートでデータの

送信を行うことが可能な電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法を提供することにある。

【００１７】

【課題を解決するための手段】

本発明の電子機器ネットワークシステムは、上記の課題を解決するために、ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおいて、上記電子機器、記憶手段および外部機器は、それぞれがセキュリティ機能を有していることを特徴としている。

【００１８】

上記の構成によれば、電子機器から記憶手段を介して外部機器へデータを送信する場合には、ユーザが希望するセキュリティレベルに対応するセキュリティ機能を有する記憶手段および外部機器を選択することで、データを安全かつ容易に記憶手段および外部機器に対して送信できる。

【００１９】

すなわち、本発明の電子機器ネットワークシステムは、電子機器と、各種データが記憶（格納）される記憶手段と、記憶手段に格納されたデータを取得して処理を行う外部機器とが、ネットワークを介して互いに接続されており、例えば、ＢMLinkS等の規格に適合した構成である。

【００２０】

電子機器は、例えば、ホストＰＣやスキャナ装置等であって、ネットワークを介して、記憶手段、外部機器に対してデータを送信する。

【００２１】

記憶手段は、例えば、ネットワーク内に設けられたストレージサーバ等であって、それぞれ個別のセキュリティレベルが設定されている。

【００２２】

外部機器は、例えば、プリンタ、ＭＦＰ（MultiFunction Printer）等であって、送信されたデータの処理を行う。

【００２３】

本発明の電子機器ネットワークシステムでは、上記電子機器、記憶手段および外部機器のそれぞれがセキュリティ機能を備えている。

【００２４】

このセキュリティ機能は、例えば、データ通信時に用いる暗号化プロトコルであってもよいし、イントラネットとインターネットとを組み合わせたネットワークを形成することでセキュリティ機能を付与してもよい。また、セキュリティレベルは、例えば、０，１，２という３段階で設定してもよい。なお、セキュリティレベル０とは、データのセキュリティについて何も考慮されていない状態でデータの送受信を行うことをいう。

【００２５】

これにより、ユーザは、送信するデータの重要度に応じてセキュリティレベルを設定し、該セキュリティレベルに基づいてデータを出力する外部機器までのデータ送信ルートを検索することで、ユーザは安全かつ確実にデータを所望の記憶手段あるいは外部機器に対して送信できる。

【００２６】

例えば、ユーザにとって重要度の高いデータを送信する場合には、セキュリティレベルが「高」である記憶手段と外部機器とを組み合わせたデータ送信ルートに沿ってデータを送信することにより、第三者にデータが漏洩する等の問題を解決できる。

【００２７】

よって、ユーザは、重要なデータを安全に送信したい場合には、ＩＤやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【００２８】

上記電子機器、記憶手段および外部機器が有しているセキュリティ機能のセキュリティレベルに応じて、上記電子機器、記憶手段および外部機器を検索する検索手段を備えていることがより好ましい。

【００２９】

これにより、ユーザは送信するデータの重要度に応じて、セキュリティレベルを設定するだけで、ネットワークに接続された複数の記憶手段、外部機器の中から、設定されたセキュリティレベルに対応する記憶手段および外部機器を容易に検索することができる。

【００３０】

よって、ユーザは、所望のセキュリティレベルのセキュリティ機能を有する記憶手段と外部機器とを組み合わせたルートに沿って、データを安全に送信することができる。

【００３１】

上記外部機器の設置場所または外部機器が備えている機能に基づいて、上記外部機器の検索を行う検索手段を備えていることがより好ましい。

【００３２】

これにより、ユーザは、データを出力する外部機器が設置されている場所や外部機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができる。

【００３３】

例えば、ユーザがデータの出力を希望する地域が決まっている場合には、まず、外部機器の設置場所を入力して外部機器を検索し、該検索結果に対してさらにセキュリティレベル、外部機器が備えている機能等の条件に基づいて検索することで、ユーザの希望に沿う外部機器の検索が可能になる。

【００３４】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【００３５】

上記検索手段は、上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【００３６】

これにより、ユーザは、所望のセキュリティレベルあるいは外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの送信ルートを検索することができる。

【００３７】

例えば、ユーザがセキュリティレベル「高」でのデータ送信を希望する場合には、セキュリティレベルが「高」以上のセキュリティ機能を備えた記憶手段および外部機器を検索し、これらを組み合わせた送信ルートを検索結果として表示する。

【００３８】

よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせて送信ルートを決定する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【００３９】

上記外部機器は、自機のセキュリティレベルに対応する記憶手段を検索する検索部を備えていることがより好ましい。

【００４０】

これにより、ユーザが操作している外部機器においても、その外部機器に対してデータの送信が可能なセキュリティ機能を有する記憶手段を検索することができるため、ユーザは外部機器において、直接データが格納されている記憶手段から必要なデータを取得することが可能になる。

【００４１】

よって、外部機器において、記憶手段からデータを取得する場合でも、データの安全性を考慮した出力が可能になる。

【００４２】

また、ユーザが操作中の外部機器に対してデータを送信することができる記憶手段を検索することで、セキュリティレベルが合わないため、記憶手段に格納されたデータを目的とする外部機器から取り出すことができないといった問題を未然に防止することができる。

【００４３】

上記電子機器は、上記検索手段による検索条件を入力し、該検索結果を表示する表示手段を備えていることがより好ましい。

【００４４】

これにより、ユーザは検索条件を容易に入力できるとともに、検索結果としてセキュリティレベル、ストレージの使用料金、外部機器の設置場所、外部機器の機能等を表示することができ、ユーザの操作性を向上することができる。

【００４５】

上記電子機器、記憶手段および外部機器のセキュリティ機能は、アクセス制御手段を介して接続された複数のネットワークのうち、どのネットワークに配置されているかによって付与されることがより好ましい。

【００４６】

これにより、例えば、ルータ、ファイアウォール等のアクセス制御手段を介して接続された企業内のイントラネットと外部の誰からもアクセスが可能なインターネットとを組み合わせることで、上記企業の社員から見て、３段階のセキュリティレベルを設定することができる。具体的には、企業内に形成されたイントラネットのみに接続可能な機器等はセキュリティレベルを「高」、両方のネットワークに接続可能な機器等はセキュリティレベルを「中」、そしてインターネットのみに接続可能な機器等がセキュリティレベルを「低」とすることができる。

【００４７】

よって、ユーザは、重要なデータについては、社内のイントラネットのみに接続可能な機器を用いて印刷データを送信、出力することで、インターネットにしか接続できない外部の機器に対してデータが漏洩することを防止し、安全かつ確実にデータを出力することができる。

【００４８】

上記外部機器は、画像形成装置であることがより好ましい。

【００４９】

これにより、ホストＰＣ等の電子機器から送信された印刷データを、ネットワークに接続された複数の記憶手段、外部機器の中から、ユーザ所望のセキュリテ

ィレベルに適合した記憶手段、画像形成装置に対して送信することができるため、データの安全性を確保した印刷システムを構築できる。

【００５０】

上記電子機器は、スキャナ装置であることがより好ましい。

【００５１】

これにより、スキャナ装置で読み取った画像データ等を、記憶手段、外部機器あるいは他の電子機器に対して安全に送信することが可能なスキャナシステムを構築できる。

【００５２】

本発明の電子機器ネットワークシステムによるデータ送信先検索方法は、上記の課題を解決するために、ネットワークを介してデータを送信する電子機器と、該電子機器から送信されたデータを記憶する複数の記憶手段と、該記憶手段から上記データを取得して処理を行う複数の外部機器とが、ネットワークを介して互いに接続されている電子機器ネットワークシステムにおけるデータ送信方法において、上記電子機器、記憶手段および外部機器は、それぞれセキュリティ機能を有しており、上記電子機器からデータを送信する場合には、ユーザが設定したセキュリティレベルに応じて、該セキュリティレベルに適合するセキュリティ機能を備えた上記記憶手段および外部機器の検索を行うことを特徴としている。

【００５３】

上記の方法によれば、ネットワークを介して複数の電子機器、記憶手段および外部機器がそれぞれ分散配置されたBMLinkS等に適合した電子機器ネットワークシステムにおいて、ユーザが希望するセキュリティレベルに応じて、適合する記憶手段および外部機器を検索できるため、ネットワークに接続された多数の記憶手段および外部機器の中から、安全にデータを送信できる記憶手段および外部機器を容易に見つけることができる。

【００５４】

すなわち、本発明に係る電子機器ネットワークシステムは、電子機器と、各種データが記憶（格納）される記憶手段と、記憶手段に格納されたデータを取得して処理を行う外部機器とが、ネットワークを介して互いに接続されており、例え

ば、BMLinkS等の規格に適合した構成である。

【００５５】

電子機器は、例えば、ホストＰＣやスキャナ装置等であって、ネットワークを介して、記憶手段、外部機器に対してデータを送信する。

【００５６】

記憶手段は、例えば、ネットワーク内に設けられたストレージサーバ等であって、それぞれ個別のセキュリティレベルが設定されている。

【００５７】

外部機器は、例えば、プリンタ、ＭＦＰ（MultiFunction Printer）等であって、送信されたデータの処理を行う。

【００５８】

また、本発明に係る電子機器ネットワークシステムでは、上記電子機器、記憶手段および外部機器のそれぞれがセキュリティ機能を備えている。

【００５９】

このセキュリティ機能は、例えば、暗号化プロトコルを用いたデータ通信であってもよいし、イントラネットおよびインターネットを組み合わせたネットワークを形成することでセキュリティ機能を付与してもよい。また、セキュリティレベルは、例えば、０，１，２という３段階に設定してもよい。なお、セキュリティレベル０とは、データのセキュリティについて何も考慮されていない状態でデータの送受信を行うことをいう。

【００６０】

これにより、ユーザは、送信するデータの重要度に応じて、データを出力する外部機器までのデータ送信ルートを検索することで、ユーザは安心してデータを外部機器まで送信できる。

【００６１】

例えば、ユーザにとって重要度の高いデータを送信する場合には、セキュリティレベルの高い記憶手段と、該セキュリティレベルの高い記憶手段からデータを取得して出力可能なセキュリティレベルの外部機器とを組み合わせたデータ送信ルートに沿ってデータを送信することにより、第三者にデータが漏洩する等の問

題を解決できる。

【００６２】

よって、ユーザは、重要なデータを安全に送信したい場合には、ＩＤやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【００６３】

上記外部機器の検索は、外部機器の設置場所、機能に基づいて行われることがより好ましい。

【００６４】

これにより、ユーザは、データを出力する外部機器が設置されている場所や外部機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができる。

【００６５】

例えば、ユーザがデータの出力を希望する地域が決まっている場合には、まず、外部機器の設置場所を入力して外部機器を検索し、該検索結果に対してさらにセキュリティレベル、外部機器が備えている機能等の条件に基づいて検索することで、ユーザの希望に沿う外部機器の検索が可能になる。

【００６６】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【００６７】

上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【００６８】

これにより、ユーザは、所望のセキュリティレベル、外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの

送信ルートを検索することができる。

【００６９】

例えば、ユーザがセキュリティレベル「高」でのデータ送信を希望する場合には、セキュリティレベルが「高」以上のセキュリティ機能を備えた記憶手段および外部機器を検索し、これらを組み合わせた送信ルートを検索結果として表示する。

【００７０】

よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせて送信ルートを決定する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【００７１】

セキュリティレベルが合致しない上記電子機器、上記記憶手段および上記外部機器に対するデータの送信を禁止することがより好ましい。

【００７２】

これにより、ユーザが安全性を重視してデータ送信を行いたい場合でも、誤って誰でもアクセス可能な記憶手段や、誰でも利用可能な外部機器にデータが送信されることを防止でき、より確実にセキュリティ機能を持った所望の外部機器に対してデータを送信できる。

【００７３】

上記外部機器から上記記憶手段に格納されたデータを取り出す際に、必要なデータが格納されている記憶手段とセキュリティレベルが合致せずに該外部機器に対してデータを送信できない場合には、上記検索手段が、上記必要なデータが格納されている記憶手段とセキュリティレベルが適合する外部機器を検索することがより好ましい。

【００７４】

これにより、ユーザがある外部機器から、記憶手段に格納されているデータを取り出して出力する場合であって、必要なデータが格納されている記憶手段とセキュリティレベルが合致しない場合には、検索手段が該外部機器に対して出力可能な外部機器を検索することができる。

【００７５】

よって、ユーザは常に必要なデータを取り出せる外部機器を把握して、必要なデータをセキュリティレベルの合致した外部機器から出力することができる。

【００７６】

【発明の実施の形態】

〔実施形態１〕

本発明の電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法の一実施形態に係る印刷システムについて、図１～図１１を用いて説明すれば以下のとおりである。

【００７７】

本実施形態の印刷システムは、複数のホストＰＣ（電子機器）、複数のストレージ（記憶手段）および複数のプリンタ（外部機器）を備え、それぞれがインターネットを介して接続されたネットワークを構成している。

【００７８】

具体的には、図２に示すように、３台のホストＰＣ（ホストＨＡ１１、ホストＨＢ１２、ホストＨＣ１３）、３つのストレージ（ストレージＳＡ２１、ストレージＳＢ２２、ストレージＳＣ２３）、４台のプリンタ（プリンタＰＡ３１、プリンタＰＢ３２、プリンタＰＣ３３、プリンタＰＤ３４）、および検索サーバ（検索手段）４１とを備えている。

【００７９】

ホストＰＣ１１～１４は、例えば、パーソナルコンピュータ、ワークステーション等の一般的なコンピュータであって、プリンタ３１～３４に対して印刷データを送信する。

【００８０】

ストレージ２１～２３は、ホストＰＣ１１～１４から送信された各種データを記憶（格納）している。本実施形態のストレージ２１～２３は、特に、ホストＰＣ１１～１４から送信された印刷データを一時的に保管し、必要に応じてプリンタ３１～３４へ出力する。

【００８１】

プリンタ３１～３４は、ストレージ２１～２３から送信された、あるいはホストＰＣ１１～１４から直接送信された印刷データの出力処理、つまり印刷を行う。

【００８２】

検索サーバ４１は、各ストレージ２１～２３および各プリンタ３１～３４が有する各種の機能に基づいて、目的とするストレージ２１～２３あるいはプリンタ３１～３４を検索することができる。より具体的には、あるデータについて両面印刷で出力処理を行いたい場合に、この検索サーバ４１において、両面印刷機能を有しているプリンタ３１～３４を検索することができる。なお、この検索サーバ４１は、各ストレージ２１～２３および各プリンタ３１～３４のセキュリティレベルについても検索することができる。

【００８３】

ここで、各ホスト１１～１４、各ストレージ２１～２３および各プリンタ３１～３４に付与されたセキュリティ機能について説明する。

【００８４】

本実施形態の印刷システムでは、各ホストＰＣ１１～１４、各ストレージ２１～２３および各プリンタ３１～３４に対して、「暗号化プロトコル２．０」、「暗号化プロトコル１．０」、「暗号化プロトコルなし」という３種類のデータ保護機能を各機器ごとに付与することで、「高」、「中」、「低」の３段階のセキュリティレベルを実現している。

【００８５】

なお、セキュリティ機能を付与する方法としては、暗号化プロトコルを用いた方法に限定されるものではなく、例えば、実施形態２で説明するイントラネットとインターネットとを組み合わせて付与する方法や、実施形態３で説明する暗号化手段でデータを暗号化した状態で送信する方法であってもよい。

【００８６】

続いて、ホストＰＣ１１～１４、ストレージ２１～２３、プリンタ３１～３４、検索サーバ４１のより詳細な構成について、図１を用いて説明する。

【００８７】

各ストレージ２１～２３は、図１に示すように、通信部２１１、制御部２１２、ストレージ情報記憶部２１３、暗号・復号化部２１４および印刷データ記憶部２１５を備えている。

【００８８】

通信部２１１は、外部の各機器とのデータの送受信を行うインターフェース部である。

【００８９】

制御部２１２は、装置全体を制御する装置の中心となる部分である。

【００９０】

ストレージ情報記憶部２１３には、例えば、セキュリティレベル、使用料金などのストレージ情報が記憶されている。なお、ここに記憶されている情報については、図示しない表示手段によって表示され、ユーザが確認することができる。

【００９１】

暗号・復号化部２１４は、ストレージ２１～２３に格納される印刷データを保護するために、ホストＰＣ１１～１４から送信された印刷データの内容が、第三者によって容易に読み取られないように、印刷データの暗号化処理を行うとともに、暗号化されている印刷データを読み取り可能な状態に復元する復号化処理も行う。

【００９２】

印刷データ記憶部２１５は、上記暗号・復号化部２１４によって処理された印刷データを格納している。

【００９３】

プリンタ３１～３４は、それぞれに、通信部３１１、制御部３１２、プリンタ情報記憶部３１３、暗号・復号化部３１４、画像形成部３１５および検索部３１６を備えている。

【００９４】

通信部３１１は、外部の各機器とのデータの送受信を行うインターフェース部である。

【００９５】

制御部３１２は、装置全体を制御する装置の中心となる部分である。

【００９６】

プリンタ情報記憶部３１３は、自プリンタのプリンタ情報（例えば、セキュリティレベル、印刷機能など）を記憶している。なお、ここに記憶されている情報についても、図示しない表示手段によって表示され、ユーザが確認することができる。

【００９７】

暗号・復号化部３１４は、上記ストレージ２１～２３が備えている暗号・復号化部２１４と同様に、印刷データの暗号化処理を行うとともに、暗号化されている印刷データを読み取り可能な状態に復元する復号化処理も行う。

【００９８】

画像形成部３１５は、暗号・復号化部３１４によって復元された印刷データに基づいて画像形成を行う。

【００９９】

検索部３１６は、自プリンタに対して出力可能なストレージを検索する。

【０１００】

ホストＰＣ１１～１４は、それぞれ、通信部１１１、制御部１１２、ホスト情報記憶部１１３、暗号・復号化部１１４、検索ドライバ１１５およびプリンタドライバ１１６を備えている。

【０１０１】

通信部１１１は、外部の各機器とのデータの送受信を行うインターフェース部である。

【０１０２】

制御部１１２は、装置全体を制御する装置の中心となる部分である。

【０１０３】

ホスト情報記憶部１１３は、セキュリティレベルなどの自ホストのホスト情報を記憶している。なお、ここに記憶されている情報についても、図示しない表示手段によって表示され、ユーザが確認することができる。

【０１０４】

暗号・復号化部１１４は、上記暗号・復号化部２１４・３１４と同様に、印刷データの暗号化処理を行うとともに、暗号化されている印刷データを読み取り可能な状態に復元する復号化処理も行う。

【０１０５】

検索ドライバ１１５は、検索サーバ４１を駆動するための駆動手段であり、これを用いることで、ホストＰＣ１１～１４において、検索サーバ４１を利用して目的とする機器の検索を行うことができる。

【０１０６】

プリンタドライバ１１６は、ホストＰＣ１１～１４にインストールされているアプリケーションを用いてユーザが作成したデータを、各プリンタ用のプリントデータに変換したり、処理を依頼するプリンタに対して所望の印刷条件（部数、用紙サイズ等）で印刷処理を行わせたりする。さらに、プリンタドライバ１１６は、プリントデータ（プリントジョブ）をストレージ２１～２３へ記憶させる役割も担う。

【０１０７】

検索サーバ４１は、通信部４１１、制御部４１２、機器情報記憶部４１３および検索部４１４を備えている。

【０１０８】

通信部４１１は、外部の各機器とのデータの送受信を行うインターフェース部である。

【０１０９】

制御部４１２は、検索サーバ４１を制御する装置の中心となる部分である。

【０１１０】

機器情報記憶部４１３は、本ネットワークにおける全ての機器に関する情報、例えば、各プリンタやストレージのセキュリティレベル、各プリンタの印刷機能等を記憶している。なお、ここに記憶されている情報についても、ホストＰＣの図示しない表示部によって表示され、ユーザに確認させることができる。

【０１１１】

検索部４１４は、ユーザから指定された検索内容に応じて、ネットワーク上の

各機器から情報を取得した機器情報記憶部４１３に記憶されている機器情報に基づいて、ユーザ所望のセキュリティ機能を有するホストＰＣ１１～１４、ストレージ２１～２３あるいはプリンタ３１～３４の検索を行う。

【０１１２】

各ストレージ２１～２３、各プリンタ３１～３４、各ホストＰＣ１１～１４、検索サーバ４１にそれぞれ設けられている各情報記憶部１１３・２１３・３１３・４１３は、図３（ａ）～図３（ｄ）に示すように、各種情報を記憶している。

【０１１３】

ストレージ２１～２３がそれぞれ備えているストレージ情報記憶部２１３は、図３（ａ）に示すように、ストレージ名、ストレージ使用料金およびセキュリティレベル（データ保護機能）を記憶している。

【０１１４】

ストレージＳＡ２１は、セキュリティレベルが「高」であり、印刷データを暗号化して送信することができる暗号化プロトコル２．０、およびサーバトラブル時対策のためのバックアップ機能を備えている。

【０１１５】

ストレージＳＢ２２は、セキュリティレベルが「中」であり、印刷データを暗号化して送信することができる暗号化プロトコル１．０を備えている。

【０１１６】

また、ストレージサーバＳＣ２３は、セキュリティレベルが「低」であって、データ保護目的の機能を特に備えていない。

【０１１７】

本実施形態の印刷システムでは、以上のように、データ保護に関するセキュリティレベルの異なる３つのストレージを備えている。

【０１１８】

ここで、セキュリティレベル「高」とは、ネットワーク的にも、物理的にもデータ保護の観点から安全性が高いストレージを意味する。このセキュリティレベル「高」のストレージとしては、例えば、会社内のイントラネット上にある機器（パソコン、プリンタなど）としか接続できないストレージがある。

【０１１９】

セキュリティレベル「中」とは、ネットワーク的な面では安全性に問題があるが、物理的には安全性が高いストレージを意味する。このセキュリティレベル「中」のストレージとしては、例えば、会社内に設置されているが、社外のインターネット上にある機器と接続できるストレージがある。

【０１２０】

セキュリティレベル「低」のストレージとは、ネットワーク的な面からも、物理的な面からもデータ保護の面である程度の危険性を有するストレージを意味する。このセキュリティレベル「低」のストレージとしては、例えば、インターネット上で誰でもアクセス可能なストレージサービスがある。

【０１２１】

なお、上述したイントラネット、インターネット等を組み合わせてセキュリティ機能が付与されたストレージを備えた印刷システムについては、後述する実施形態２において詳しく説明する。

【０１２２】

上記のように、各ストレージ２１～２３は、そのセキュリティレベルに差があるため、使用料金について、そのセキュリティレベルに応じて高いものから順に２００円、１００円、無料と設定されている。

【０１２３】

各プリンタ３１～３４のプリンタ情報記憶部３１３は、図３（ｂ）に示すように、プリンタ名、各プリンタ３１～３４のセキュリティレベルを示すデータ保護機能、プリンタの設置場所およびプリンタが備えている印刷機能について記憶している。

【０１２４】

プリンタＰＡ３１は、暗号化プロトコル２．０および１．０、および印刷される直前まで暗号化された状態で印刷データをストックすることができるように復号化機能を備えており、セキュリティレベルは「特高」である。

【０１２５】

プリンタＰＢ３２は、暗号化プロトコル２．０および１．０を備えており、セ

キュリティレベルは「高」である。

【０１２６】

プリンタＰＣ３３は、暗号化プロトコル１．０のみを備えており、セキュリティレベルは「中」である。

【０１２７】

プリンタＰＤ３４は、データ保護目的の機能を特に備えておらず、セキュリティレベルは「低」である。

【０１２８】

また、プリンタ情報記憶部３１３は、各プリンタの設置場所および各プリンタが備えているカラー、両面、ステープル等の印刷機能に関する情報も記憶している。この記憶情報については、各プリンタの図示しない表示部、あるいは検索サーバ４１を介して、各ホストＰＣから確認することができる。

【０１２９】

各ホストＰＣ１１～１４のホスト情報記憶部１１３は、図３（ｃ）に示すように、ホスト名と、各ホストＰＣ１１～１４のセキュリティレベルを示すデータ保護機能とに関する情報を記憶している。

【０１３０】

本実施形態の各ホストＰＣ１１～１４は、印刷データを暗号化して送信することができる暗号化プロトコル２．０および１．０を全て備えており、セキュリティレベル「低」、「中」、「高」の全てのレベルに対応可能である。

【０１３１】

検索サーバ４１の機器情報記憶部４１３は、図３（ｄ）に示すように、ストレージ名、接続可能なプリンタおよびセキュリティレベルに関する情報を記憶している。

【０１３２】

これらの情報は、検索サーバ４１が、各プリンタ３１～３４からプリンタ情報、各ストレージ２１～２３からストレージ情報をそれぞれ収集することにより取得してもよいし、予め作成された情報を記憶しておいてもよい。

【０１３３】

本実施形態の印刷システムにおいては、検索サーバ４１がこのような機器情報記憶部４１３を備えていることにより、各印刷データに対して付与すべきセキュリティレベルに応じて、各種機器（ストレージ２１～２３、プリンタ３１～３４）を選択することができる。

【０１３４】

なお、検索サーバ４１には、図４（ａ）～図４（ｃ）に示すように、各セキュリティレベルに応じて、ストレージとプリンタとを組み合わせた印刷ルートを検索する図示しないルート検索部（ルート検索手段）が設けられていてもよい。

【０１３５】

例えば、ユーザ所望のセキュリティレベルが「高」以上（「特高」または「高」）である場合には、検索サーバ４１は、図４（ａ）に示すように、ストレージＳＡ２１と、プリンタＰＡ３１またはプリンタＰＢ３２とを組み合わせた印刷ルートを検索することができる。

【０１３６】

ユーザ所望のセキュリティレベルが「中」の場合には、図４（ｂ）に示すように、ストレージＳＢ２２と、プリンタＰＡ３１またはプリンタＰＢ３２またはプリンタＰＣ３３とを組み合わせた印刷ルートを検索することができる。

【０１３７】

ユーザ所望のセキュリティレベルが「低」の場合には、検索サーバ４１は、図４（ｃ）に示すように、ストレージＳＣ２３と、プリンタ３１～３４のうちの任意のプリンタとを組み合わせた印刷ルートを検索することができる。

【０１３８】

本実施形態の印刷システムは、このように、ユーザが希望するセキュリティレベルに応じて、最適な送信ルートを容易に検索することができるため、データ保護のセキュリティ面を考慮してホストＰＣ１１～１４から送信された印刷データをプリンタ３１～３４において出力することができる。

【０１３９】

次に、本実施形態の印刷システムにおいて、セキュリティレベルに応じた印刷データの送信方法について、図５および図６（ａ）～図６（ｄ）を用いて説明す

れば以下のとおりである。

【０１４０】

なお、図６（ａ）～図６（ｄ）は、各ホストＰＣ１１～１４において、印刷処理を行う場合に表示される操作画面を示す模式図である。

【０１４１】

ホストＰＣ１１～１４において印刷データ送信を開始する場合には、図５に示すように、Ｓ１において、最初にホストＰＣ１１～１４の検索ドライバ１１５が起動する。これにより、Ｓ２において、該ホストＰＣ１１～１４と検索サーバ４１とが接続される。

【０１４２】

すると、ホストＰＣ１１～１４には、図６（ａ）に示すような表示画面が現れ、検索カテゴリー（検索条件）を選択することができる。

【０１４３】

ここで、セキュリティレベルに応じた検索を行う場合には、Ｓ３において、「セキュリティ」ボタンを選択する。

【０１４４】

続いて、ホストＰＣ１１～１４には、図６（ｂ）に示すような表示画面が現れ、所望とするセキュリティレベル（その印刷データに付与したいセキュリティレベル）を選択することができる。なお、図６（ｂ）には、セキュリティレベル「高」を選択した場合を示す。

【０１４５】

Ｓ４において、例えば、セキュリティレベル「高」が選択されると、Ｓ５において、図６（ｃ）に示すように、目的とするセキュリティレベルに応じたストレージが表示される。

【０１４６】

そして、Ｓ６において、ユーザは図６（ｃ）に示されるような３つのストレージから任意のストレージを選択する。なお、図６（ｃ）には、ストレージＳＡが選択された場合を示す。

【０１４７】

Ｓ６において、ユーザが所望のストレージを選択すると、Ｓ７において、図６（ｄ）に示すように、先に選択したストレージとセキュリティレベルとに応じて、印刷可能なプリンタが表示される。

【０１４８】

ここで、表示された印刷可能プリンタの設置場所あるいは印刷機能が目的とするものでない場合、すなわち、Ｓ８においてＹｅｓの場合には、再度Ｓ３より操作をやり直すことができる。

【０１４９】

一方、上記印刷可能プリンタの機能等が目的に適合したものである場合、すなわち、Ｓ８でＮｏの場合には、Ｓ９において、ストレージ使用料として課金処理が行われた後、Ｓ１０において、印刷データが作成される。そして、Ｓ１１において、該当するストレージへ暗号化プロトコルを利用して印刷データが送信される。

【０１５０】

本実施形態の印刷システムでは、以上のように、ホストＰＣからストレージに対して印刷データが送信されるため、印刷データのセキュリティレベルに応じたルートで送信処理を行うことができ、データ保護の観点から安全性の高い印刷システムを実現できる。

【０１５１】

次に、本実施形態の印刷システムにおいて、印刷データを出力するプリンタの設置場所を優先して印刷データの送信ルートを決定する方法について、図７に示すフローチャートを用いて説明すれば以下のとおりである。

【０１５２】

上述した印刷データの送信方法では、セキュリティレベルの設定を優先して印刷ルートを決定していたが、ここでは、印刷データの出力処理が行われるプリンタの設置場所の設定を優先して、プリンタとストレージとを組み合わせた印刷ルートを検索する。

【０１５３】

ホストＰＣ１１～１４から印刷データの送信を開始する場合には、図７に示す

ように、Ｓ２１において、最初に、ホストＰＣ１１～１４内の検索ドライバ１１５を起動し、Ｓ２２において、該ホストＰＣ１１～１４を検索サーバ４１に接続する。

【０１５４】

すると、ホストＰＣ１１～１４における図示しない表示部には、図８（ａ）に示すような表示画面が現れ、検索カテゴリー（検索条件）を選択することができる。ここで、印刷データを出力するプリンタの選択を優先して検索を行う場合には、Ｓ２３において、「プリンタ」ボタンを選択する。

【０１５５】

続いて、ホストＰＣ１１～１４の表示部には、図８（ｂ）に示すような表示画面が現れ、ユーザは、Ｓ２４において、例えば、設置場所、機能などのプリンタの検索条件を入力する。なお、図８（ｂ）には、検索条件として、プリンタの設置場所（住所）を選択した場合を示す。

【０１５６】

ここで、例えば、ユーザが、印刷を行いたいプリンタの設置場所（住所）として、奈良県を選択した場合には、Ｓ２５において、図８（ｃ）に示すように、奈良県内に設置されたプリンタの一覧が表示される。なお、この一覧には、プリンタの設置場所だけでなく、印刷機能およびセキュリティレベルについても表示される。

【０１５７】

従って、ユーザは、Ｓ２６において、希望する設置場所およびその印刷データに見合った印刷機能およびセキュリティレベルを備えたプリンタを選択することができる。なお、Ｓ２６において、ユーザの希望に見合ったプリンタが一覧に表示されていない場合には、再度、Ｓ２３に戻って検索カテゴリーの選択からやり直すこともできる。

【０１５８】

Ｓ２６において、プリンタが選択されると、Ｓ２７において、印刷データの出力処理が行われる。Ｓ２７における出力処理は、ストレージ２１～２３に一時的に印刷データを格納した後、プリンタ３１～３４へ送信されて出力される場合と

、ストレージ２１～２３を介さず直接プリンタ３１～３４において出力が行われる場合とに分けられる。

【０１５９】

先ず、印刷データがストレージ２１～２３を介さず、直接プリンタ３１～３４に送信されて出力される場合について説明する。

【０１６０】

この場合には、Ｓ３３において、該当するプリントの使用料に応じた課金処理が行われた後、Ｓ３４において、印刷データが作成される。そして、上記印刷データは、Ｓ３５において、該当するプリンタ３１～３４へ送信され印刷処理が行われる。

【０１６１】

次に、印刷データが、ストレージ２１～２３に一時的に格納された後、プリンタ３１～３４へ送信されて出力される場合について説明する。

【０１６２】

この場合は、図８（ｃ）に示す表示画面において、「ストレージへ出力」というボタンを選択する。すると、ホストＰＣ１１～１４の表示部には、図８（ｄ）に示すように、Ｓ２８において、選択されたプリンタ３１～３４に対して出力可能なストレージ２１～２３を表示する画面が現れる。よって、ユーザは、Ｓ２９において、その印刷データに見合ったセキュリティレベルおよび料金を備えたストレージを選択することができる。なお、Ｓ２９において、ユーザが希望するストレージが一覧にない場合には、再度、Ｓ２３に戻って検索カテゴリーの選択からやり直すこともできる。

【０１６３】

Ｓ２９において、ストレージが選択されると、Ｓ３０において、選択されたプリンタおよびストレージの使用料に応じた課金処理が行われた後、印刷データが作成される。そして、印刷データは、Ｓ３２において、選択されたストレージへ送信される。

【０１６４】

本実施形態の印刷システムでは、以上のような方法により、ホストＰＣ１１～

１４からストレージまたはプリンタに対して印刷データの送信が行われることで、ユーザの希望する場所に設置されたプリンタにおいて印刷データを出力できる。さらに、印刷データの重要度に応じて、セキュリティレベルの異なる複数の印刷データの送信ルートから最適なルートを選択することができるため、操作性に優れ、かつ印刷データ保護の観点から安全性の高い印刷システムを実現できる。

【０１６５】

さらに、本実施形態の印刷システムにおいて、各ストレージが持つ機能を優先してストレージを検索し、印刷データの送信ルートを決定する方法について、図９のフローチャートを用いて説明すれば以下のとおりである。

【０１６６】

ホストＰＣ１１～１４から印刷データの送信を開始する場合には、図９に示すように、Ｓ４１において、最初にホストＰＣ１１～１４内の検索ドライバ１１５を起動させ、Ｓ４２において、該ホストＰＣ１１～１４を検索サーバ４１に接続する。

【０１６７】

すると、ホストＰＣ１１～１４の図示しない表示部には、図１０（ａ）に示すような表示画面が現れ、検索カテゴリー（検索条件）を選択することができる。

【０１６８】

ここで、ストレージのセキュリティレベルを優先して検索を行う場合には、Ｓ４３において、「ストレージ」ボタンを選択する。

【０１６９】

続いて、ホストＰＣ１１～１４の表示部には、図１０（ｂ）に示すような表示画面が現れ、ユーザは、Ｓ４４において、例えば、名前、セキュリティなどのストレージ２１～２３の検索条件を入力する。なお、図１０（ｂ）では、検索条件として、ストレージ２１～２３の「名前」を選択した場合を示している。

【０１７０】

ここで、例えば、ストレージＳＣ２３が選択されると、Ｓ４５において、図１０（ｃ）に示すような表示画面が現れる。あるいは、Ｓ４５において、ストレージＳＡ２１が選択されると、図１０（ｄ）に示すような表示画面が現れる。

【０１７１】

そして、図１０（ｃ）または図１０（ｄ）に示す表示画面に表示されたストレージＳＡ２１またはストレージＳＣ２３に対応する出力可能なプリンタ、ストレージとプリンタとの組合せ（ルート）によって定まるセキュリティレベル、および出力に要する料金が、その印刷データに見合ったものであれば、図１０（ｃ）または図１０（ｄ）において「ＯＫ」ボタンを選択し、Ｓ４６において、ストレージの選択を行う。

【０１７２】

ここで、出力可能プリンタ、セキュリティレベルおよび料金等が、ユーザの希望するものでない場合には、再度、Ｓ４３に戻って、検索カテゴリーの選択からやり直すことができる。

【０１７３】

Ｓ４６において、ユーザの希望するストレージが選択されると、Ｓ４７において、該当するストレージの使用料に応じた課金処理が行われた後、Ｓ４８において、印刷データが作成される。そして、Ｓ４９において、上記印刷データは該当するストレージへ送信される。

【０１７４】

本実施形態の印刷システムは、以上のように、ホストＰＣ１１～１４からストレージ２１～２３に対して印刷データが送信されることにより、所望のセキュリティレベルのストレージに対して印刷データの送信し、該印刷データを記憶することができる。さらに、印刷データの重要度に応じて、セキュリティレベルの異なる複数の送信ルートの中から最適なルートを選択することができるため、操作性に優れ、かつデータ保護の観点から安全性の高い印刷システムを実現できる。

【０１７５】

さらに、本実施形態に係る印刷システムにおいては、プリンタ３１～３４から、検索サーバ４１を用いて所望のセキュリティレベルのストレージを検索し、該検索されたストレージに蓄積された印刷データを取得することもできる。以下に、プリンタ３１～３４からストレージ２１～２３を検索する方法について、図１１に示すフローチャートを用いて説明する。

【０１７６】

任意のプリンタから印刷データの検索を開始する場合には、図１１に示すように、Ｓ６１において、最初にプリンタ３１～３４における図示しない検索ドライバを起動し、Ｓ６２において、該プリンタを検索サーバ４１に接続する。

【０１７７】

すると、プリンタの表示部には、上段にて説明した図１０（ａ）に示す検索カテゴリーを表示する画面が現れ、検索カテゴリー（検索条件）を選択することができる。

【０１７８】

ここで、ストレージに応じた検索を行う場合には、Ｓ６３において、「ストレージ」ボタンを選択する。

【０１７９】

続いて、プリンタの表示部上には、図１０（ｂ）に示す表示画面が現れ、ユーザは、Ｓ６４において、例えば、名前、セキュリティレベルなどのストレージの検索条件を入力する。すると、Ｓ６５において、プリンタの表示部にはその検索結果が表示され、Ｓ６６において、ユーザは目的とする印刷データが格納されているストレージを選択することができる。なお、再度、検索条件の選択をやり直したい場合は、Ｓ６３に戻ることも可能である。

【０１８０】

Ｓ６６において、目的とする印刷データが格納されているストレージを選択すると、Ｓ６７において、その印刷データが当該プリンタにおいて印刷可能であるか否かについて判断される。すなわち、ここでは、現在ユーザが操作を行っているプリンタに対して、セキュリティの面で、所望の印刷データが格納されたストレージからデータを取得することが可能であるか否かについて判断される。

【０１８１】

Ｓ６７で印刷可能と判断された場合、すなわちＹｅｓが選択された場合には、Ｓ６８において、検索したストレージから印刷データを取得できる。そして、Ｓ６９において印刷が行われた後、Ｓ７０において、使用料金に応じた課金処理が行われて、処理が終了する。

【０１８２】

一方、Ｓ６７において印刷不可能と判断された場合、すなわちＮｏが選択された場合には、Ｓ７１において、その旨が表示部によって報知される。そして、Ｓ７２において、ユーザは、印刷可能なプリンタを再度検索するか否かを選択することができる。Ｓ７２において、再検索を行うことを選択した場合、すなわちＹｅｓを選択した場合には、Ｓ７３において、印刷可能なプリンタの検索を行うことができる。また、Ｓ７２において、再検索を行わないことを選択した場合、すなわちＮｏが選択された場合には、処理を終了する。

【０１８３】

本実施形態の印刷システムでは、以上のように、プリンタと印刷データが格納されているストレージとのセキュリティレベルが一致せず、かつプリンタのセキュリティレベルがストレージのセキュリティレベルよりも低い場合には、そのストレージからプリンタに対して印刷データを送信することができない。

【０１８４】

これにより、印刷データが記憶されているストレージよりもセキュリティレベルが低いプリンタから、誤ってセキュリティレベルの高い印刷データを出力する等の問題の発生を防止し、印刷データの安全性を確保できる。

【０１８５】

また、上記のように、セキュリティレベルの不適合により、必要な印刷データが格納されているストレージからプリンタに対して該印刷データの送信ができない場合には、ユーザが操作しているプリンタの検索部３１６によって、該ストレージとセキュリティレベルが合致したプリンタを検索することができる。このため、ユーザは、操作中のプリンタ以外に、セキュリティレベルの合致したプリンタをすぐに把握でき、設置場所、機能等の条件が合えば、その新たに検索されたプリンタから印刷データを出力することができる。

【０１８６】

なお、本実施形態では、ホストＰＣについてセキュリティレベルは特に設定されていなかったが、本発明はこれに限定されるものではなく、ホストＰＣについても、ストレージやプリンタと同様に、セキュリティレベルが設定されていても

よい。

【０１８７】

〔実施形態２〕

本発明の電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法の他の実施形態に係る印刷システムについて、図１２～図１４（ｃ）を用いて説明すれば以下のとおりである。なお、説明の便宜上、上記実施形態１にて説明した図面と同じ機能を有する部材については、同じ符号を付記し、その説明を省略する。

【０１８８】

本実施形態の印刷システムは、基本的な構成としては、上記実施形態１におけるネットワークと同様である。しかし、本実施形態におけるネットワークでは、ネットワークの一部が、会社内など狭い範囲内での通信を可能にするイントラネットを介して接続されている点で異なっている。

【０１８９】

本実施形態の印刷システムが接続されているネットワークにおいては、図１２に示すように、ホストＨＡ１１、ストレージＳＡ２１、プリンタ３１が、イントラネット６０上でのみ接続可能な機器である。

【０１９０】

また、ホストＨＢ１２、ストレージＳＢ２２、プリンタ３２は、イントラネット６０およびインターネット６１の双方から接続可能な機器である。なお、検索サーバ４１についても、イントラネット６０およびインターネット６１の両方のネットワークに接続されているホストＰＣおよびプリンタから接続することができる。

【０１９１】

ホストＨＣ１３、ホストＨＤ１４、プリンタＰＣ３３、ストレージＳＣ２３およびプリンタＰＤ３４は、インターネット６１上でのみ接続することができる機器である。

【０１９２】

なお、図１２において斜線で囲まれた領域、すなわちイントラネット６０およ

びインターネット６１の双方から接続可能なネットワーク６２と、イントラネット６０上のネットワークとの双方に含まれる各機器は、データ保護（セキュリティ）の観点から、データ保安用のシステムであるルータ（アクセス制御手段）４２を介してイントラネット６０内の他の機器と接続されている。また、図１２において斜線で囲まれた領域、すなわちインターネット６１とイントラネット６０との双方に含まれるネットワーク６２に配置された機器は、同じくデータ保護（セキュリティ）の観点から、データ保安用のシステムであるfirewall（アクセス制御手段）４３を介して、インターネット６１内の他の機器と接続されている。

【０１９３】

ホストＰＣ１１～１４のホスト情報記憶部１１３には、図１３（ａ）に示すように、各ホストＰＣ１１～１４の接続可能なストレージおよびその設置場所が記憶されている。この接続可能なストレージについては、図１２に示すネットワークの構成により決定される。例えば、ホストＨＣ１３については、イントラネット６０内のストレージＳＢ２２とも接続できるようになっている。

【０１９４】

プリンタ３１～３４のプリンタ情報記憶部３１３には、図１３（ｂ）に示すように、各プリンタ３１～３４の接続可能ストレージが記憶されている。この接続可能ストレージについては、上記と同様に、図１２に示すネットワーク構成により決定される。例えば、プリンタＰＣ３３については、ストレージＳＢ２２とも接続できるようになっている。また、プリンタ情報記憶部３１３には、各プリンタの設置場所、および、各プリンタが備えているカラー、両面、ステープルなどの印刷機能に関する情報も記憶されている。この記憶情報については、各プリンタの図示しない表示部、あるいは検索サーバ４１を介して、各ホストＰＣから確認することができる。

【０１９５】

ストレージ２１～２３のストレージ情報記憶部２１３には、図１３（ｃ）に示すように、各ストレージ２１～２３の接続可能ホスト、接続可能プリンタ、設置場所が記憶されている。上記接続可能ホスト、および上記接続可能プリンタについては、図１２に示すネットワーク構成に示す通りであるが、ストレージＳｂ２

２については、インターネット６１上のホストＨＣ１３およびプリンタＰＣ３３と接続できるようになっている。

【０１９６】

検索サーバ４１の機器情報記憶部４１３には、図１３（ｄ）に示すように、各ストレージＳＡ～ＳＣが接続可能なホストＨＡ～ＨＤおよびプリンタＰＡ～ＰＤが記憶されているとともに、各ホスト、各ストレージを介して各プリンタにおいて印刷処理を行った場合のセキュリティレベルが記憶されている。

【０１９７】

本実施形態の印刷システムでは、このような機器情報記憶部４１３を備えた検索サーバ４１を備えることによって、各印刷データの重要度に応じてセキュリティレベルを設定し、そのセキュリティレベルに対応する各種機器（ストレージ、プリンタ）を選択して処理を行うことができる

このように、本実施形態の印刷システムでは、図１３（ｄ）に示すように、その印刷データのセキュリティレベルが異なる３つの印刷ルート（すなわち、ストレージ、ホスト、プリンタの組合せ）が存在する。

【０１９８】

なお、セキュリティレベル「高」とは、ネットワーク的にも、物理的にもデータ保護の観点からも高い安全性を有するものを意味している。本実施形態の印刷システムにおけるセキュリティレベル「高」の印刷ルートとしては、例えば、会社内のイントラネット６０上にある機器のみを経由するルートがある。

【０１９９】

また、セキュリティレベル「中」とは、ネットワーク的な面では安全性に問題があるが、物理的には高い安全性を有するものを意味している。本実施形態の印刷システムにおけるセキュリティレベル「中」の印刷ルートとしては、例えば、会社内に設置されているホストおよびプリンタを用いているが、社外のインターネット６１上にあるホスト、プリンタ、ストレージとも接続できる印刷ルートがある。

【０２００】

さらに、セキュリティレベル「低」とは、ネットワーク的な面からも、物理的

な面からもデータ保護の観点から危険性を有するもののことを意味している。本実施形態の印刷システムにおいて、セキュリティレベル「低」の印刷ルートとしては、例えば、インターネット６１上で誰でもアクセスすることが可能な機器を経由するルートがある。

【０２０１】

なお、本実施形態の印刷システムが備えている検索サーバ４１には、図１４（ａ）～図１４（ｃ）に示すように、各セキュリティレベルに応じて、ストレージとプリンタとを組み合わせて構成される印刷ルートを検索する図示しないルート検索部（ルート検索手段）が設けられていてもよい。

【０２０２】

例えば、所望のセキュリティレベルが「高」以上の場合には、図１４（ａ）に示すように、ホストＨＡ１１またはホストＨＢ１２を選択し、ストレージＳＡ２１を選択し、プリンタＰＡ３１またはプリンタ３２ＰＢを選択する印刷ルートが検索される。

【０２０３】

また、所望のセキュリティレベルが「中」の場合には、図１４（ｂ）に示すように、ホストＨＡ１１、ホストＨＢ１２、ホストＨＣ１３の何れかのホストＰＣと、ストレージＳＢ２２と、プリンタＰＡ３１、プリンタＰＢ３２、プリンタＰＣ３３の何れかのプリンタとを選択する印刷ルートが検索される。

【０２０４】

また、所望のセキュリティレベルが「低」の場合には、図１４（ｃ）に示すように、ホストＨＢ１２、ホストＨＣ１３、ホストＨＤ１４の何れかのホストＰＣと、ストレージＳＣ２３と、プリンタＰＣ３３、プリンタＰＤ３４の何れかのプリンタとを選択する印刷ルートが検索される。

【０２０５】

本実施形態の印刷システムは、以上のように、検索機能を備えているため、所望のセキュリティレベルに応じた印刷ルートを容易に検索することがき、効率よく印刷ルートを選択できる。

【０２０６】

なお、本実施形態の印刷システムにおいて実行されるセキュリティレベルに応じた印刷データの送信については、上述の実施形態１に記載の方法と同様にして実行することができるため、説明を省略する。

【０２０７】

〔実施形態３〕

本実施形態の電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法のさらに他の実施形態に係るスキャナシステムについて、図１５～図１８を用いて説明すれば以下のとおりである。なお、説明の便宜上、上記実施形態１にて説明した図面と同じ機能を有する部材については、同じ符号を付記し、その説明を省略する。

【０２０８】

本実施形態のスキャナシステムは、図１に示すホストＰＣ（外部機器）１１～１４、ストレージ２１～２３、プリンタ３１～３４および検索サーバ（検索手段）４１に加えて、図１５に示すような、スキャナ（電子機器）５１～５４を備えている。そして、スキャナ５１～５４からスキャンデータをホストＰＣに対してデータを送信する点で、ホストＰＣ１１～１４からプリンタ３１～３４に対して印刷データを送信する上記実施形態１・２と異なっている。

【０２０９】

スキャナ５１～５４は、通信部５１１、制御部５１２、スキャナ情報記憶部５１３、暗号化部５１４、検索部５１５、操作部５１６および画像読取部５１７を備えている。

【０２１０】

通信部５１１は、外部の各機器とのデータの送受信を行うインターフェース部である。

【０２１１】

制御部５１２は、スキャナ装置全体を制御する装置の中心となる部分である。

【０２１２】

スキャナ情報記憶部５１３は、スキャナ装置の設置場所、機能、セキュリティレベルなどのスキャナ装置に関する情報を記憶している。なお、ここに記憶され

ている情報についても、図示しない表示手段によって表示され、ユーザが確認することができる。

【０２１３】

暗号化部５１４は、スキャンデータを保護するために、スキャンデータの内容が第三者によって容易に読み取られないように、スキャンデータの暗号化処理を行う。

【０２１４】

検索部５１５は、セキュリティレベル等に応じて、ネットワークに接続されているストレージやプリンタの検索を行う。

【０２１５】

操作部５１６は、ユーザが直接スキャナ装置を操作する際に使用され、ユーザからの指示を入力する。

【０２１６】

画像読取部５１７は、スキャナ機能によって原稿を読み取り、画像データとして取り込む。

【０２１７】

各ストレージ２１～２３、各プリンタ３１～３４、各ホストＰＣ１１～１４、検索サーバ４１における各情報記憶部１１３・２１３・３１３・４１３は、図１６（ａ）～図１６（ｄ）に示すように、各種情報を記憶している。

【０２１８】

各ストレージ２１～２３におけるストレージ情報記憶部２１３は、図１６（ａ）に示すように、ストレージ名、ストレージ使用料金およびセキュリティレベルを示すデータ保護機能を記憶している。

【０２１９】

例えば、ストレージＳＡ２１は、セキュリティレベルが「高」であり、スキャンデータを暗号化して送信することができる暗号化プロトコル２．０という暗号化保護機能を備えている。

【０２２０】

ストレージＳＢ２２は、セキュリティレベルが「中」であり、スキャンデータ

を暗号化して送信することができる暗号化プロトコル１．０を備えている。

【０２２１】

ストレージサーバＳＣ２３は、セキュリティレベルが「低」であって、データ保護目的の機能を特に備えていない。

【０２２２】

本実施形態のスキャンシステムでは、実施形態１の図３と同様に、データ保護に関するセキュリティレベルの異なる３つのストレージを備えている。

【０２２３】

次に、各スキャナ５１～５４におけるスキャナ情報記憶部５１３は、図１６（ｂ）に示すように、スキャナ名、セキュリティレベルを示すデータ保護機能、スキャナの設置場所、および各スキャナが備えているスキャナ機能について記憶している。

【０２２４】

スキャナＳｃＡ５１は、暗号化プロトコル２．０および１．０、暗号化機能を備えており、セキュリティレベルは「特高」である。

【０２２５】

スキャナＳｃＢ５２は、暗号化プロトコル２．０および１．０を備えており、セキュリティレベルは「高」である。

【０２２６】

スキャナＳｃＣ５３は、暗号化プロトコル１．０のみを備えており、セキュリティレベルは「中」である。

【０２２７】

スキャナＳｃＤ５４は、データ保護目的の機能を特に備えておらず、セキュリティレベルは「低」である。

【０２２８】

また、スキャナ情報記憶部５１３は、各スキャナの設置場所および各スキャナが備えているカラー、モノクロおよび解像度等のスキャナ機能に関する情報についても記憶している。この記憶情報については、各スキャナの図示しない表示部、あるいは検索サーバ４１を介して、各ホストＰＣから確認することができる。

【０２２９】

各ホストＰＣ１１～１４のホスト情報記憶部１１３は、図１６（ｃ）に示すように、ホスト名と、各ホストＰＣ１１～１４のセキュリティレベルを示すデータ保護機能と、データ暗号復号機能の有無に関する情報とを記憶している。

【０２３０】

本実施形態の各ホストＰＣ１１～１４は、スキャンデータを暗号化して送信することができる暗号化プロトコル２．０および１．０を備えており、暗号化プロトコルを備えていないホストＨＤ１４を含めて、セキュリティレベル「低」から「高」までの全てのレベルに対応可能である。

【０２３１】

検索サーバ４１の機器情報記憶部４１３は、図１６（ｄ）に示すように、ルート、暗号化プロトコルの有無、データ暗号化の有無、およびセキュリティレベルに関する情報を記憶している。

【０２３２】

これらの情報は、検索サーバ４１が、各スキャナ５１～５４からスキャナ情報、各ストレージ２１～２３からストレージ情報、各ホストＰＣ１１～１４からホスト情報をそれぞれ収集することにより取得してもよいし、予め作成された情報を記憶しておいてもよい。

【０２３３】

本実施形態のスキャナシステムにおいては、検索サーバ４１がこのような機器情報記憶部４１３を備えていることにより、各スキャナ５１～５４から、各スキャンデータに対して付与すべきセキュリティレベルに応じて、各機器（ストレージ２１～２３、ホストＰＣ１１～１４）を選択することができる。

【０２３４】

なお、検索サーバ４１には、図１７（ａ）～図１７（ｆ）に示すように、各セキュリティレベルに応じて、スキャナとストレージとホストＰＣとを組み合わせたデータの送信ルートを検索する図示しないルート検索部（ルート検索手段）が設けられていてもよい。

【０２３５】

例えば、ユーザ所望のセキュリティレベルが「特高」である場合には、検索サーバ４１は、図１７（ａ）に示すように、スキャナＳｃＡ５１と、ストレージＳＡ２１と、ホストＨＡ１１とを組み合わせたデータの送信ルートであって、かつ暗号化した状態でデータを送信するルートを検索することができる。

【０２３６】

具体的には、スキャナにおいて、スキャンデータの暗号化を行い、ストレージにおいてスキャンデータの暗号化はそのままで、暗号化プロトコル２．０を用いて送信し、ホストＰＣにおいてデータ利用時に復号化すればよい。

【０２３７】

また、ユーザ所望のセキュリティレベルが「高」である場合には、検索サーバ４１は、図１７（ｂ）に示すように、スキャナＳｃＡ５１あるいはスキャナＳｃＢ５２と、ストレージＳＡ２１と、ホストＨＡ１１あるいはホストＨＢ１２とを組み合わせたデータの送信ルートを検索することができる。

【０２３８】

具体的には、スキャナからデータを暗号化プロトコル２．０で送信し、ストレージにおいて保存し、データ利用時には、ストレージにおいてデータを復号化し、暗号化プロトコル２．０でホストＰＣへ送信すればよい。

【０２３９】

また、ユーザ所望のセキュリティレベルが同じく「高」である場合には、検索サーバ４１は、図１７（ｃ）に示すように、スキャナＳｃＡ５１と、ストレージＳＢ２２と、ホストＨＡ１１あるいはホストＨＣ１３とを組み合わせたデータの送信ルートであって、かつ暗号化した状態でデータを送信するルートを検索することができる。

【０２４０】

具体的には、スキャナにおいてスキャンデータの暗号化を行い、暗号化プロトコル１．０でデータを送信し、暗号化されたままストレージにおいて保存し、データ利用時には、暗号化プロトコル１．０でデータを送信し、ホストＰＣにおいて復号化すればよい。

【０２４１】

さらに、ユーザ所望のセキュリティレベルが「中」である場合には、検索サーバ４１は、図１７（ｄ）に示すように、スキャナＳｃＡ５１あるいはスキャナＳｃＢ５２あるいはスキャナＳｃＣ５４と、ストレージＳＢ２２と、ホストＨＡ１１あるいはホストＨＢ１２あるいはホストＨＣ１３とを組み合わせたデータの送信ルートを検索することができる。

【０２４２】

具体的には、スキャナにおいてスキャンデータを暗号化プロトコル１．０で送信し、ストレージにおいて保存し、データ利用時には、暗号化プロトコル１．０でスキャンデータを送信すればよい。

【０２４３】

また、ユーザ所望のセキュリティレベルが同じく「中」である場合には、検索サーバ４１は、図１７（ｅ）に示すように、スキャナＳｃＡ５１と、ストレージＳＢ２３と、ホストＨＡ１１あるいはホストＨＣ１３とを組み合わせたデータの送信ルートであって、かつ暗号化した状態でデータを送信するルートを検索することができる。

【０２４４】

具体的には、スキャナにおいてスキャンデータを暗号化し、ノンセキュリティ通信で送信し、ストレージにおいて暗号化されたデータをそのまま保存し、暗号化されたデータをノンセキュリティ通信して、データ利用時に復号化すればよい。

【０２４５】

ユーザ所望のセキュリティレベルが「低」の場合には、検索サーバ４１は、図１７（ｆ）に示すように、スキャナＳｃＡ５１～ＳｃＤ５４の何れかのスキャナと、ストレージＳＣ２３と、ホストＨＡ１１～ＨＤ１４の何れかのホストＰＣとを組み合わせたデータの送信ルートを検索することができる。

【０２４６】

具体的には、スキャンデータをそのままノンセキュリティ通信で送信し、スキャンデータをそのまま保存し、ホストＰＣへのノンセキュリティ通信でスキャンデータを送信すればよい。

【０２４７】

本実施形態のスキャナシステムは、このように、セキュリティレベルに応じて、データの送信ルートを容易に検索することができるため、データ保護のセキュリティ面を考慮して、スキャナからホストＰＣまでデータを送信することができる。

【０２４８】

スキャナ５１～５４において、スキャンデータの送信を開始する場合には、図１８に示すように、Ｓ８１において、最初にスキャナ５１～５４の検索部５１５を起動する。これにより、Ｓ８２において、該スキャナ５１～５４と検索サーバ４１とが接続される。

【０２４９】

ここで、セキュリティレベルに応じた検索を行う場合には、Ｓ８３において、「セキュリティ」ボタンを選択する。

【０２５０】

Ｓ８４において、例えば、セキュリティレベル「高」が選択されると、Ｓ８５において、目的とするセキュリティレベルに応じたストレージが表示される。

【０２５１】

そして、Ｓ８６において、ユーザは３つのストレージから任意のストレージを選択する。

【０２５２】

Ｓ８６において、ユーザが所望のストレージを選択すると、Ｓ８７において、先に選択したストレージとセキュリティレベルとに応じて、接続可能なホストＰＣが表示される。

【０２５３】

ここで、表示された接続可能なホストＰＣの設置場所あるいは機能がユーザの希望に合致するものでない場合、すなわち、Ｓ８８においてＹｅｓの場合には、再度Ｓ８３より操作をやり直すことができる。

【０２５４】

一方、上記接続可能ホストＰＣの機能、セキュリティレベル等が、ユーザの希

望に合致するものである場合、すなわち、Ｓ８８においてＮｏの場合には、Ｓ８９において、ストレージ使用料として課金処理が行われた後、Ｓ９０において、スキャンが開始される。そして、暗号化プロトコルを利用してスキャンデータの暗号化処理がされた後、Ｓ９１において、該当するストレージへの送信が行われる。

【０２５５】

本実施形態のスキャナシステムでは、以上のように、スキャナからストレージに対してスキャンデータが送信されるため、スキャンデータのセキュリティレベルに応じたルートでスキャンデータの送信処理を行うことができ、データ保護の観点から安全性の高いスキャナシステムを実現できる。

【０２５６】

また、上記実施形態１・２のように、ホストＰＣからストレージ、プリンタに対してデータを送信してもよいし、本実施形態のように、スキャナ装置等の電子機器からストレージ、ホストＰＣ、その他の外部機器等へデータを送信してもよい。

【０２５７】

さらに、図１７（ａ）、図１７（ｃ）および図１７（ｅ）に示すように、スキャナ、ストレージ、ホストＰＣのそれぞれが有している暗号化プロトコル等の通信データ保護機能と、データの暗号化とを組み合わせることにより、ユーザが選択可能なデータ送信ルートの選択肢を増やすことができる。

【０２５８】

なお、上述した実施形態１～３において説明した電子機器ネットワークシステムは、本発明の一例であって、本発明は上記各実施形態の記載に限定されるものではない。例えば、より多くのホストＰＣ、ストレージ、プリンタを備えた印刷システムに対しても適用可能である。さらに、印刷システム以外にも、実施形態３で説明したスキャナ等のようなプリンタ以外の電子機器を用いてネットワークを構成した電子機器ネットワークシステムであってもよい。

【０２５９】

また、上記各実施形態１～３では、電子機器（ホストＰＣ、スキャナ）、外部

機器（プリンタ、ホストＰＣ）および記憶手段（ストレージ）のそれぞれについてセキュリティレベルを付与した例をあげて説明したが、本発明はこれに限定されるものではない。例えば、ユーザにもセキュリティレベルが設定されており、上記実施形態１～３で説明した電子機器、外部機器および記憶手段等と組み合わせてもよい。これにより、機密性の高いデータについては、特定のユーザに限ってセキュリティレベルが「特高」の機器を利用できるようにすれば、さらに安全性が高い電子機器ネットワークシステムを構築できる。

【０２６０】

本発明は上述した各実施形態に限定されるものではなく、請求項に示した範囲で種々の変更が可能であり、異なる実施形態にそれぞれ開示された技術的手段を適宜組み合わせて得られる実施形態についても本発明の技術的範囲に含まれる。

【０２６１】

本発明は、ホストＰＣから送られた印刷データを記憶する複数のストレージと、上記ストレージから該印刷データを取得し印刷を行う複数のプリンタとを備えた印刷システムにおいて、上記複数のストレージは、ストレージごとにセキュリティレベルが異なり、上記印刷システムは、ユーザにとって指定された上記印刷データのセキュリティレベルに応じて、当該印刷データが格納されるストレージを検索する検索手段をさらに備えることを特徴とする電子機器ネットワークシステムと表現することもできる。

【０２６２】

本発明は、ホストＰＣから送られた印刷データを記憶する複数のストレージと、上記ストレージから該印刷データを取得し印刷を行う複数のプリンタとを備えた印刷システムにおいて、ユーザによって指定された上記印刷データのセキュリティレベルに応じて、当該印刷データが格納されるストレージを検索する第１の検索手段と、上記検索手段の検索結果によって選択されたストレージのセキュリティレベルを示す表示手段と、当該ストレージから印刷データを取得し印刷可能なプリンタを検索する第２の検索手段とをさらに備えることを特徴とする印刷システムと表現することもできる。

【０２６３】

【発明の効果】

本発明の電子機器ネットワークシステムは、以上のように、電子機器、記憶手段および外部機器は、それぞれがセキュリティ機能を有している構成である。

【０２６４】

それゆえ、電子機器から記憶手段を介して外部機器へデータを送信する場合には、ユーザが希望するセキュリティレベルに対応するセキュリティ機能を有する記憶手段および外部機器を選択することで、データを安全かつ容易に記憶手段および外部機器に対して送信できるという効果を奏する。

【０２６５】

よって、ユーザは、重要なデータを安全に送信したい場合には、ＩＤやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【０２６６】

上記電子機器、記憶手段および外部機器が有しているセキュリティ機能のセキュリティレベルに応じて、上記電子機器、記憶手段および外部機器を検索する検索手段を備えていることがより好ましい。

【０２６７】

それゆえ、ユーザは送信するデータの重要度に応じて、セキュリティレベルを設定するだけで、ネットワークに接続された複数の記憶手段、外部機器の中から、設定されたセキュリティレベルに対応する記憶手段および外部機器を容易に検索することができる。よって、ユーザは、所望のセキュリティレベルのセキュリティ機能を有する記憶手段と外部機器とを組み合わせたルートに沿って、データを安全に送信することができるという効果を奏する。

【０２６８】

上記外部機器の設置場所または外部機器が備えている機能に基づいて、上記外部機器の検索を行う検索手段を備えていることがより好ましい。

【０２６９】

それゆえ、ユーザは、データを出力する外部機器が設置されている場所や外部

機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができるという効果を奏する。

【０２７０】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【０２７１】

上記検索手段は、上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【０２７２】

それゆえ、ユーザは、所望のセキュリティレベルあるいは外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの送信ルートを検索することができるという効果を奏する。よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせて送信ルートを決定する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【０２７３】

上記外部機器は、自機のセキュリティレベルに対応する記憶手段を検索する検索部を備えていることがより好ましい。

【０２７４】

それゆえ、ユーザが操作している外部機器においても、その外部機器に対してデータの送信が可能なセキュリティ機能を有する記憶手段を検索することができるため、ユーザは外部機器において、直接データが格納されている記憶手段から必要なデータを取得することが可能になるという効果を奏する。よって、外部機器において、記憶手段からデータを取得する場合でも、データの安全性を考慮した出力が可能になる。また、ユーザが操作中の外部機器に対してデータを送信することができる記憶手段を検索することで、セキュリティレベルが合わないため、記憶手段に格納されたデータを目的とする外部機器から取り出すことができな

いといった問題を未然に防止することができる。

【０２７５】

上記電子機器は、上記検索手段による検索条件を入力し、該検索結果を表示する表示手段を備えていることがより好ましい。

【０２７６】

それゆえ、ユーザは検索条件を容易に入力できるとともに、検索結果としてセキュリティレベル、ストレージの使用料金、外部機器の設置場所、外部機器の機能等を表示することができ、ユーザの操作性を向上することができるという効果を奏する。

【０２７７】

上記電子機器、記憶手段および外部機器のセキュリティ機能は、アクセス制御手段を介して接続された複数のネットワークのうち、どのネットワークに配置されているかによって付与されることがより好ましい。

【０２７８】

それゆえ、例えば、ルータ、ファイアウォール等のアクセス制御手段を介して接続された企業内のイントラネットと外部の誰からもアクセスが可能なインターネットとを組み合わせることで、上記企業の社員から見て、３段階のセキュリティレベルを設定することができる。よって、ユーザは、重要なデータについては、社内のイントラネットのみに接続可能な機器を用いて印刷データを送信、出力することで、インターネットにしか接続できない外部の機器に対してデータが漏洩することを防止し、安全かつ確実にデータを出力することができるという効果を奏する。

【０２７９】

上記外部機器は、画像形成装置であることがより好ましい。

【０２８０】

それゆえ、ホストＰＣ等の電子機器から送信された印刷データを、ネットワークに接続された複数の記憶手段、外部機器の中から、ユーザ所望のセキュリティレベルに適合した記憶手段、画像形成装置に対して送信することができるため、データの安全性を確保した印刷システムを構築できるという効果を奏する。

【０２８１】

上記電子機器は、スキャナ装置であることがより好ましい。

【０２８２】

それゆえ、スキャナ装置で読み取った画像データ等を、記憶手段、外部機器あるいは他の電子機器に対して安全に送信することが可能なスキャナシステムを構築できるという効果を奏する。

【０２８３】

本発明の電子機器ネットワークシステムによるデータ送信先検索方法は、以上のように、上記電子機器、記憶手段および外部機器は、それぞれセキュリティ機能を有しており、上記電子機器からデータを送信する場合には、ユーザが設定したセキュリティレベルに応じて、該セキュリティレベルに適合するセキュリティ機能を備えた上記記憶手段および外部機器の検索を行う構成である。

【０２８４】

それゆえ、ネットワークを介して複数の電子機器、記憶手段および外部機器がそれぞれ分散配置されたBMLinkS等に適合した電子機器ネットワークシステムにおいて、ユーザが希望するセキュリティレベルに応じて、適合する記憶手段および外部機器を検索できるため、ネットワークに接続された多数の記憶手段および外部機器の中から、安全にデータを送信できる記憶手段および外部機器を容易に見つけることができるという効果を奏する。

【０２８５】

よって、ユーザは、重要なデータを安全に送信したい場合には、ＩＤやパスワードを入力することなく、単に、所望のセキュリティレベルに合致した記憶手段および外部機器を選択するだけで、データの安全性を確保した電子機器ネットワークシステムを実現することが可能となる。

【０２８６】

上記外部機器の検索は、外部機器の設置場所、機能に基づいて行われることがより好ましい。

【０２８７】

それゆえ、ユーザは、データを出力する外部機器が設置されている場所や外部

機器が備えている機能に基づいて外部機器を検索することができるため、ネットワークに接続された複数の外部機器の中から、ユーザの希望に沿った外部機器をより容易に選択することができるという効果を奏する。

【０２８８】

また、送信されるデータの処理が特殊である場合には、外部機器の機能に基づいてその処理を行う機能を備えた外部機器を検索することができ、より詳細な検索が可能になる。

【０２８９】

上記電子機器から、上記記憶手段または上記外部機器に対して送信されるデータの送信ルートを検索することがより好ましい。

【０２９０】

それゆえ、ユーザは、所望のセキュリティレベル、外部機器の設置場所、機能等に基づいて、電子機器から記憶手段を介して外部機器に至るまでのデータの送信ルートを検索することができるという効果を奏する。よって、ユーザ所望のセキュリティレベルに応じて別々に検索した記憶手段および外部機器を組み合わせて送信ルートを決定する場合と比較して、効率よく所望のセキュリティレベルに適合する送信ルートを見つけることができる。

【０２９１】

セキュリティレベルが合致しない上記電子機器、上記記憶手段および上記外部機器に対するデータの送信を禁止することがより好ましい。

【０２９２】

それゆえ、ユーザが安全性を重視してデータ送信を行いたい場合でも、誤って誰でもアクセス可能な記憶手段や、誰でも利用可能な外部機器にデータが送信されることを防止でき、より確実にセキュリティ機能を持った所望の外部機器に対してデータを送信できるという効果を奏する。

【０２９３】

上記外部機器から上記記憶手段に格納されたデータを取り出す際に、必要なデータが格納されている記憶手段とセキュリティレベルが合致せずに該外部機器に対してデータを送信できない場合には、上記検索手段が、上記必要なデータが格

納されている記憶手段とセキュリティレベルが適合する外部機器を検索することがより好ましい。

【０２９４】

それゆえ、ユーザがある外部機器から、記憶手段に格納されているデータを取り出して出力する場合であって、必要なデータが格納されている記憶手段とセキュリティレベルが合致しない場合には、検索手段が該外部機器に対して出力可能な外部機器を検索することができるという効果を奏する。よって、ユーザは常に必要なデータを取り出せる外部機器を把握して、必要なデータをセキュリティレベルの合致した外部機器から出力することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係る印刷システムが備えているホストＰＣ、ストレージ、プリンタおよび検索サーバの構成を示すブロック図である。

【図２】

図１の印刷システムの概略的な構成を示すブロック図である。

【図３】

（ａ）～（ｄ）は、各機器における情報記憶部に記憶された記憶内容を示す図である。

【図４】

（ａ）～（ｃ）は、セキュリティレベル別のデータの送信ルートを示すブロック図である。

【図５】

図１の印刷システムによる、セキュリティレベルを優先して検索した場合の印刷データの送信ルートを検索する手順を示すフローチャートである。

【図６】

（ａ）～（ｄ）は、図５のフローチャートに示す方法によって印刷データの出力処理を行う場合における、ホストＰＣに表示される操作画面を示す図である。

【図７】

図１の印刷システムによる、プリンタを優先して検索した場合の印刷データの

送信ルートを検索する手順を示すフローチャートである。

【図８】

（ａ）～（ｄ）は、図７のフローチャートに示す方法によって印刷データの出力処理を行う場合における、ホストＰＣに表示される操作画面を示す図である。

【図９】

図１の印刷システムによる、ストレージを優先して検索した場合の印刷データの送信ルートを検索する手順を示すフローチャートである。

【図１０】

（ａ）～（ｄ）は、図９のフローチャートに示す方法によって印刷データの出力処理を行う場合に、ホストＰＣ上に表示される操作画面を示す図である。

【図１１】

図１の印刷システムにおけるプリンタからストレージを検索して印刷データを得る場合の印刷データの送信ルートを検索する手順を示すフローチャートである。

【図１２】

本発明の他の本実施形態に係る印刷システムが構築されているネットワークの構成を示すブロック図である。

【図１３】

（ａ）～（ｄ）は、各機器がそれぞれ備えている各情報記憶部が記憶している記憶内容を示す図である。

【図１４】

（ａ）～（ｃ）は、セキュリティレベルに応じた印刷データの送信ルートを示すブロック図である。

【図１５】

本発明のさらに他の実施形態に係るスキャナシステムのスキャナの内部構成を示すブロック図である。

【図１６】

（ａ）～（ｄ）は、各機器がそれぞれ備えている各情報記憶部が記憶している記憶内容を示す図である。

【図１７】

（ａ）～（ｆ）は、セキュリティレベルに応じた印刷データの送信ルートを示すブロック図である。

【図１８】

図１５のスキャナシステムにおけるスキャナからホストＰＣへデータを送信する場合の送信ルートを検索する手順を示すフローチャートである。

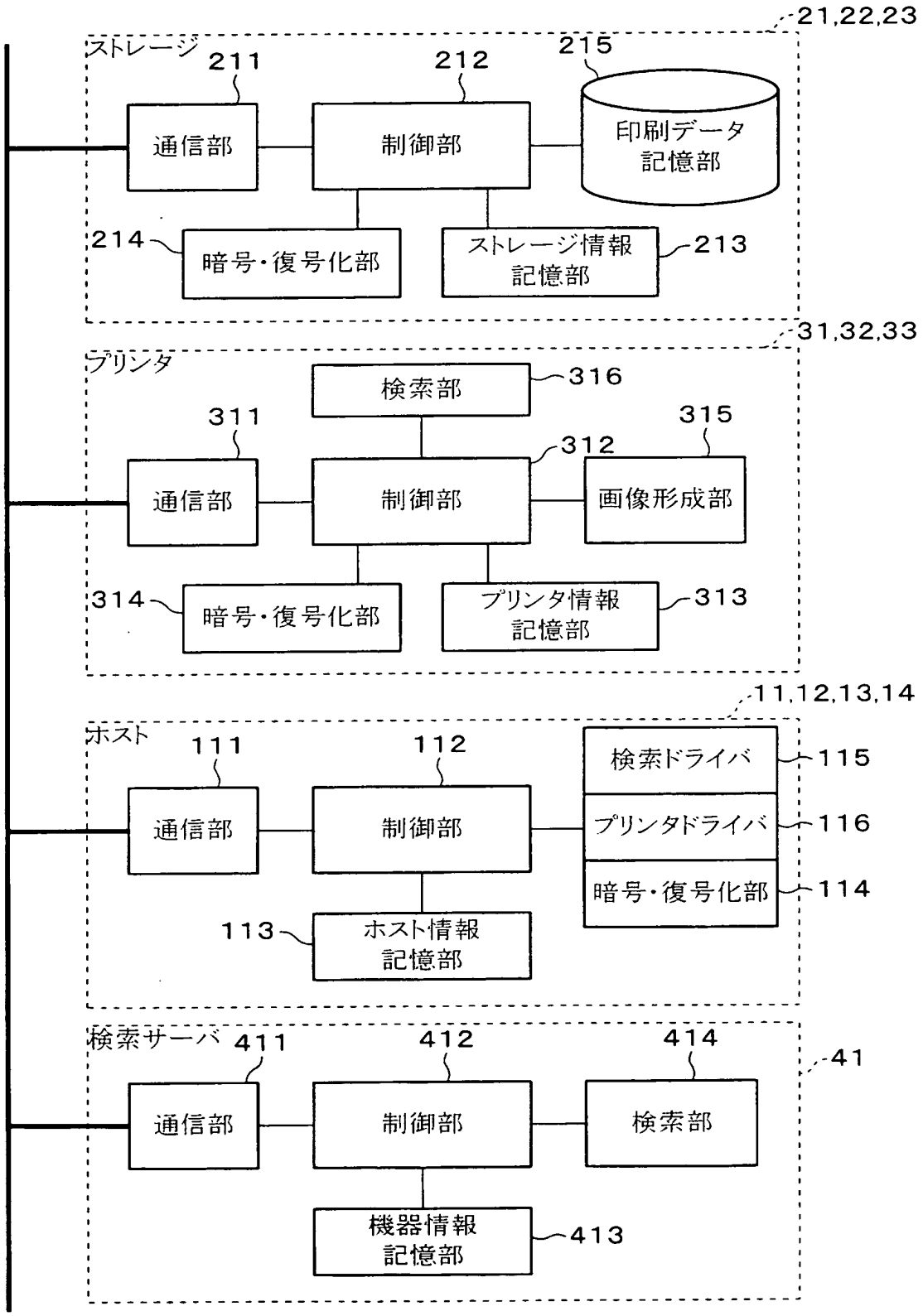
【符号の説明】

１１～１４	ホストＰＣ（電子機器、外部機器）
２１～２３	ストレージ（記憶手段）
３１～３４	プリンタ（外部機器）
４１	検索サーバ（検索手段）
４２	ルータ（アクセス制御手段）
４３	firewall（アクセス制御手段）
５１～５４	スキャナ（電子機器、外部機器）
６０	イントラネット
６１	インターネット
６２	双方から接続可能なネットワーク
１１１	通信部
１１２	制御部
１１３	ホスト情報記憶部
１１４	暗号・復号化部
１１５	検索ドライバ
１１６	プリンタドライバ
２１１	通信部
２１２	制御部
２１３	ストレージ情報記憶部
２１４	暗号・復号化部
２１５	印刷データ記憶部
３１１	通信部

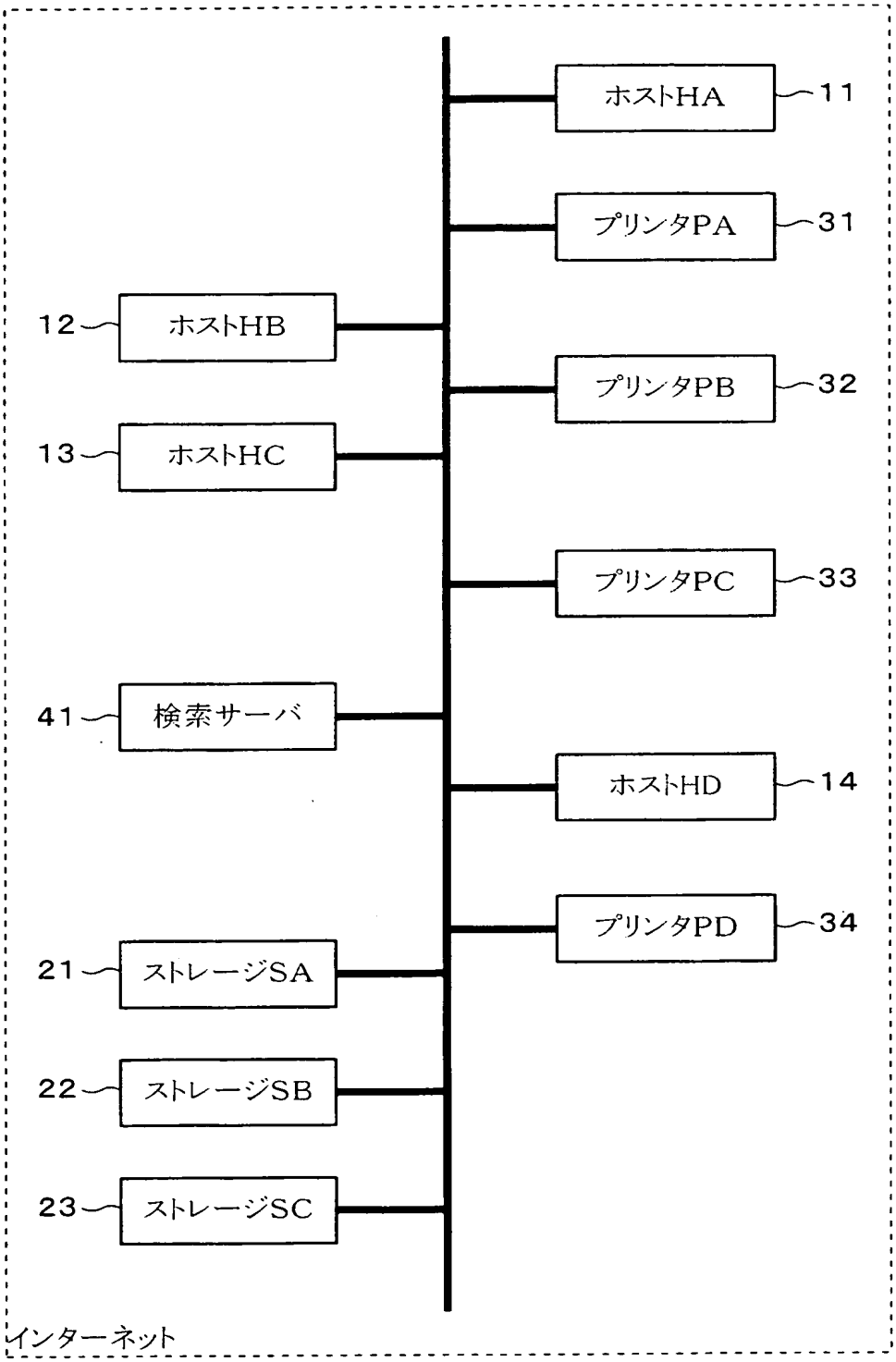
３１２　制御部
３１３　プリンタ情報記憶部
３１４　暗号・復号化部
３１５　画像形成部
３１６　検索部
４１１　通信部
４１２　制御部
４１３　機器情報記憶部
４１４　検索部
５１１　通信部
５１２　制御部
５１３　スキャナ情報記憶部
５１４　暗号化部
５１５　検索部
５１６　操作部
５１７　画像読み取り部

【書類名】　図面

【図１】


21,22,23
ストレージ
211
212
215
通信部
制御部
印刷データ
記憶部
214
暗号・復号化部
ストレージ情報
記憶部
213
31,32,33
プリンタ
検索部
316
311
315
312
通信部
制御部
画像形成部
314
暗号・復号化部
プリンタ情報
記憶部
313
11,12,13,14
ホスト
111
112
検索ドライバ
115
通信部
制御部
プリンタドライバ
116
暗号・復号化部
114
113
ホスト情報
記憶部
検索サーバ
411
412
414
41
通信部
制御部
検索部
機器情報
記憶部
413

【図２】


ホストHA
11
プリンタPA
31
12
ホストHB
プリンタPB
32
13
ホストHC
プリンタPC
33
41
検索サーバ
ホストHD
14
プリンタPD
34
21
ストレージSA
22
ストレージSB
23
ストレージSC
インターネット

【図３】

（ａ）ストレージ情報記憶部

ストレージ名	ストレージ使用料金	データ保護機能（レベル）	
ストレージSA	200円	暗号化プロトコル2.0のみ 暗号化保存、バックアップ機能	高（特高）
ストレージSB	100円	暗号化プロトコル1.0のみ	中
ストレージSC	無料	－	低

（ｂ）プリンタ情報記憶部

プリンタ名	データ保護機能（レベル）		場所	印刷機能
プリンタPA	暗号化プロトコル2.0 暗号化プロトコル1.0 復号化機能	特高	○○コンビニ 奈良店	カラー、両面
プリンタPB	暗号化プロトコル2.0 暗号化プロトコル1.0	高	○○コンビニ 天理店	両面、ステープル
プリンタPC	暗号化プロトコル1.0	中	○○コンビニ 郡山店	カラー、両面 ステープル
プリンタPD	－	低	○○コンビニ 高田店	両面、ステープル

（ｃ）ホスト情報記憶部

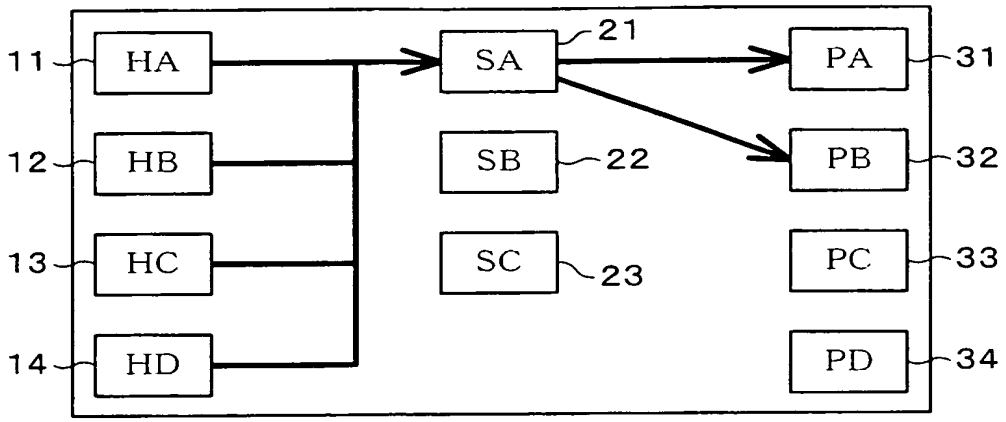
ホスト名	データ保護機能
ホストHA	暗号化プロトコル2.0 暗号化プロトコル1.0
ホストHB	暗号化プロトコル2.0 暗号化プロトコル1.0
ホストHC	暗号化プロトコル2.0 暗号化プロトコル1.0
ホストHD	暗号化プロトコル2.0 暗号化プロトコル1.0

（ｄ）機器情報記憶部

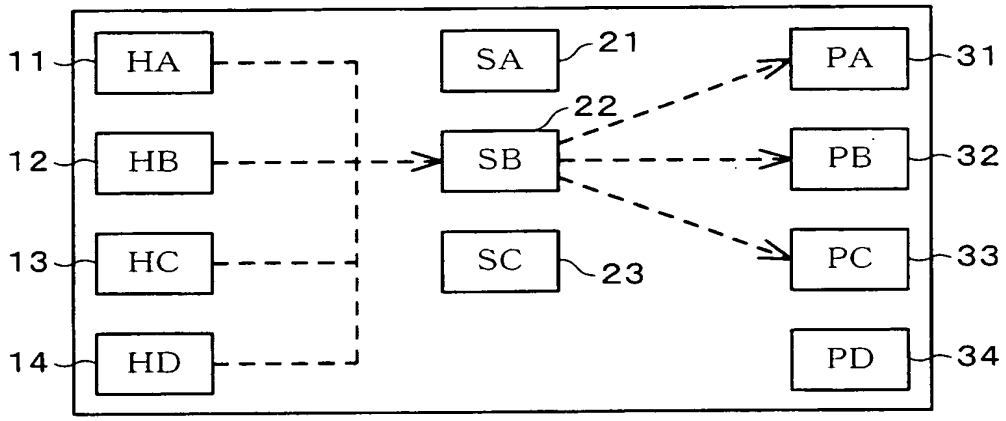
ストレージ名	接続(出力)可能プリンタ	セキュリティレベル
ストレージSA	PA	特高
ストレージSA	PB	高
ストレージSB	PA、PB、PC	中
ストレージSC	PA、PB、PC、PD	低

【図４】

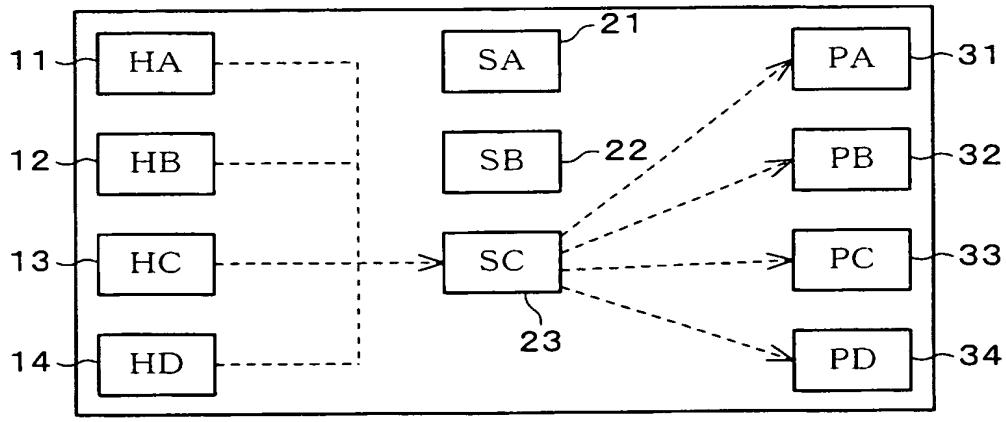
（ａ）セキュリティレベル：高



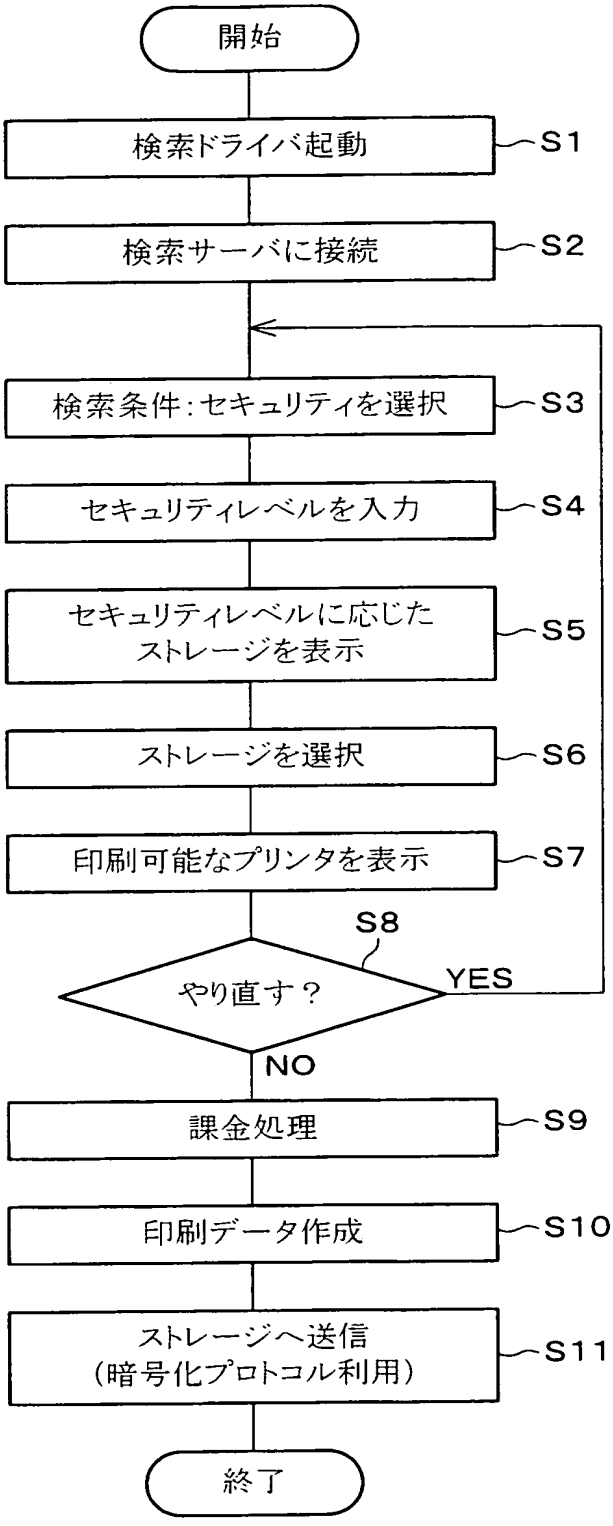
（ｂ）セキュリティレベル：中



（ｃ）セキュリティレベル：低



【図５】


開始
検索ドライバ起動
S1
検索サーバに接続
S2
検索条件：セキュリティを選択
S3
セキュリティレベルを入力
S4
セキュリティレベルに応じた
ストレージを表示
S5
ストレージを選択
S6
印刷可能なプリンタを表示
S7
S8
やり直す？
YES
NO
課金処理
S9
印刷データ作成
S10
ストレージへ送信
（暗号化プロトコル利用）
S11
終了

【図６】

（ａ）

検索カテゴリーを選択してください。

プリンタ　　ストレージ　　セキュリティ

（ｂ）

セキュリティレベルを指定して下さい。

高　　中　　低

（ｃ）

セキュリティレベル：高
ストレージが検索されました。
ストレージを選択すると、印刷可能なプリンタを検索します。

	ストレージ名	料金
1	ストレージSA	200円
2	ストレージSD	150円
3	ストレージSG	200円

ストレージ絞り込み

プリンタ条件

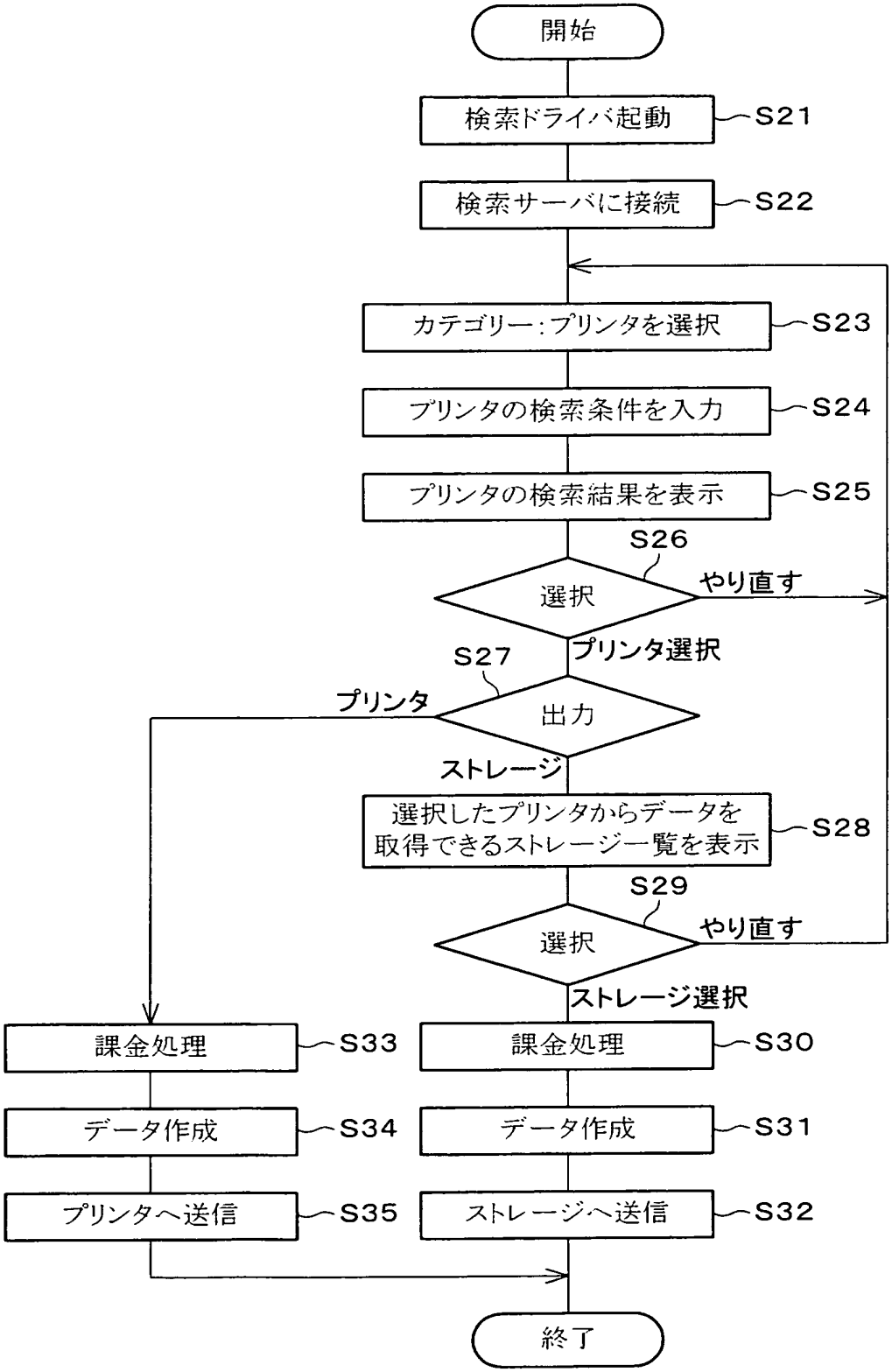
（ｄ）

セキュリティレベル：高
印刷場所：奈良県
下記のプリンタからデータを出力することが出来ます。

	プリンタ名	場所	印刷機能
ストレージSA	プリンタPA	○○コンビニ 奈良店	カラー、両面
	プリンタPB	○○コンビニ 天理店	両面、ステープル

OK　　戻る　　最初から

【図７】


開始
検索ドライバ起動
S21
検索サーバに接続
S22
カテゴリー：プリンタを選択
S23
プリンタの検索条件を入力
S24
プリンタの検索結果を表示
S25
S26
選択
やり直す
プリンタ選択
S27
プリンタ
出力
ストレージ
選択したプリンタからデータを
取得できるストレージ一覧を表示
S28
S29
選択
やり直す
ストレージ選択
課金処理
S33
課金処理
S30
データ作成
S34
データ作成
S31
プリンタへ送信
S35
ストレージへ送信
S32
終了

【図８】

（ａ）

検索カテゴリーを選択してください。

プリンタ　　ストレージ　　セキュリティ

（ｂ）

検索条件を指定して下さい。

住所　　機能　　一覧

（ｃ）

住所：奈良県
プリンタが検索されました。
プリンタを選択すると、印刷データ取得可能なストレージを検索します。

	プリンタ名	場所	印刷機能	セキュリティ
1	プリンタ PA	○○コンビニ 奈良店	カラー、両面	特高・高・中・低
2	プリンタ PB	○○コンビニ 天理店	両面、ステープル	高・中・低
3	プリンタ PC	○○コンビニ 郡山店	カラー、両面、ステープル	中・低
4	プリンタ PD	○○コンビニ 高田店	両面、ステープル	低

プリンタへ直接出力　　ストレージ出力　　戻る　　最初から

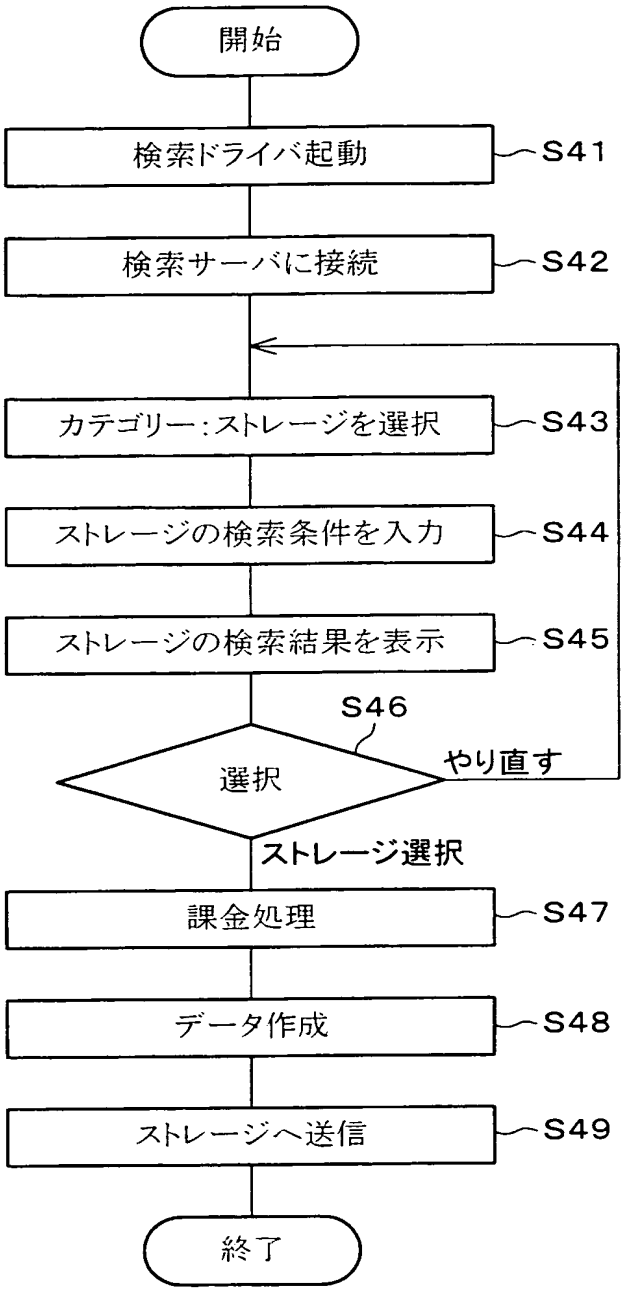
（ｄ）

プリンタ PA に出力可能なストレージです、
ストレージを選択してください。

	ストレージ名	セキュリティレベル	料金
1	ストレージ SA	高（特高）	200 円
2	ストレージ SB	中	100 円
3	ストレージ SC	低	無料

OK　　戻る　　最初から

【図９】


開始
検索ドライバ起動
S41
検索サーバに接続
S42
カテゴリー：ストレージを選択
S43
ストレージの検索条件を入力
S44
ストレージの検索結果を表示
S45
S46
選択
やり直す
ストレージ選択
課金処理
S47
データ作成
S48
ストレージへ送信
S49
終了

【図１０】

（ａ）

検索カテゴリーを選択してください。

プリンタ　　ストレージ　　セキュリティ

（ｂ）

検索条件を指定して下さい。

名前　　セキュリティ　　一覧

（ｃ）

「ストレージSC」が検索されました

	ストレージ名	出力可能プリンタ	セキュリティ	料金
1	ストレージSC	プリンタPA プリンタPB プリンタPC プリンタPD	低	無料

セキュリティレベルが「低」です。
印刷データの機密レベルが高い場合は、セキュリティレベルの高いストレージを選択することをお勧めします。

OK　　戻る　　最初から　　プリンタの詳細

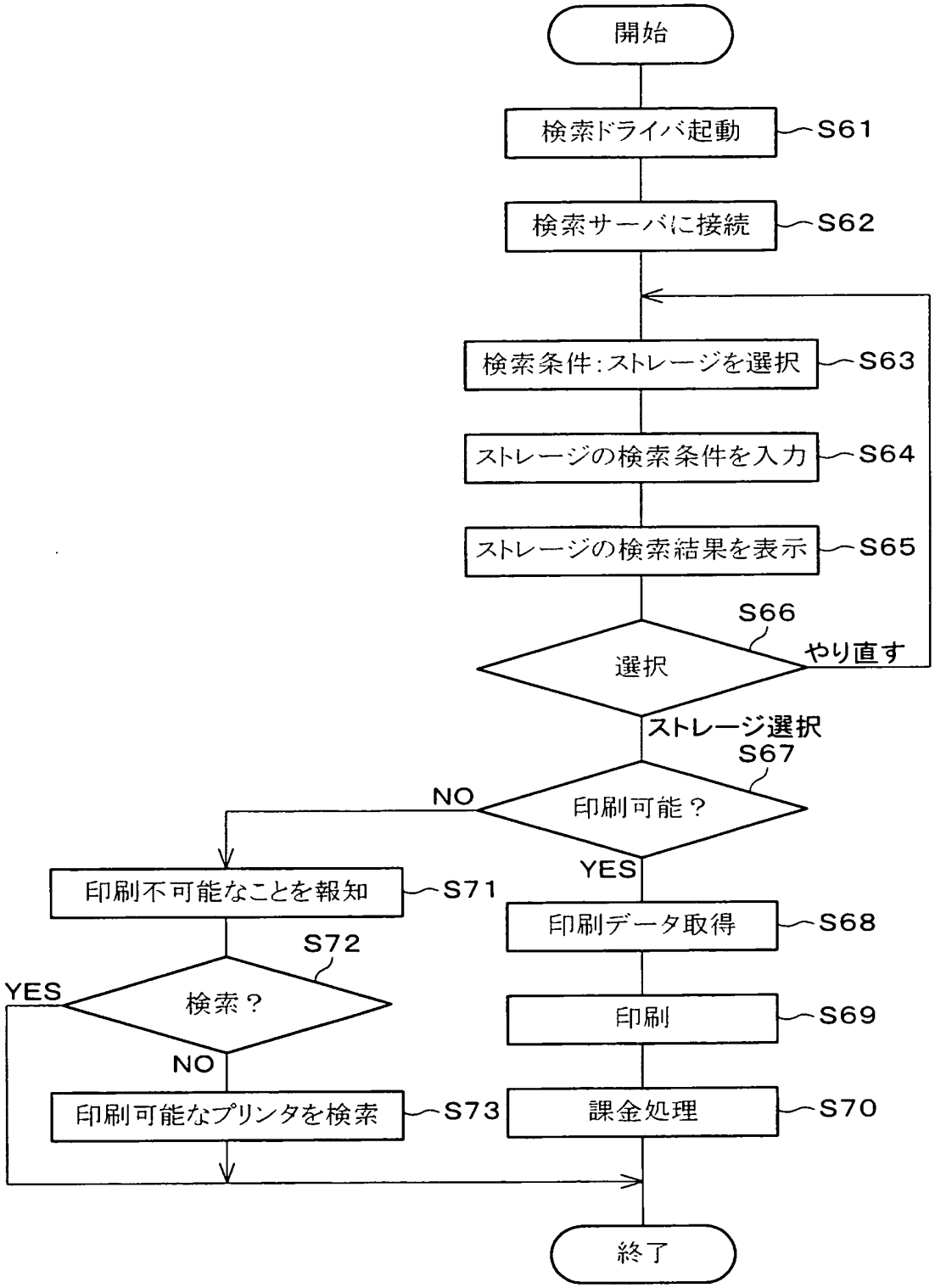
（ｄ）

「ストレージSA」が検索されました

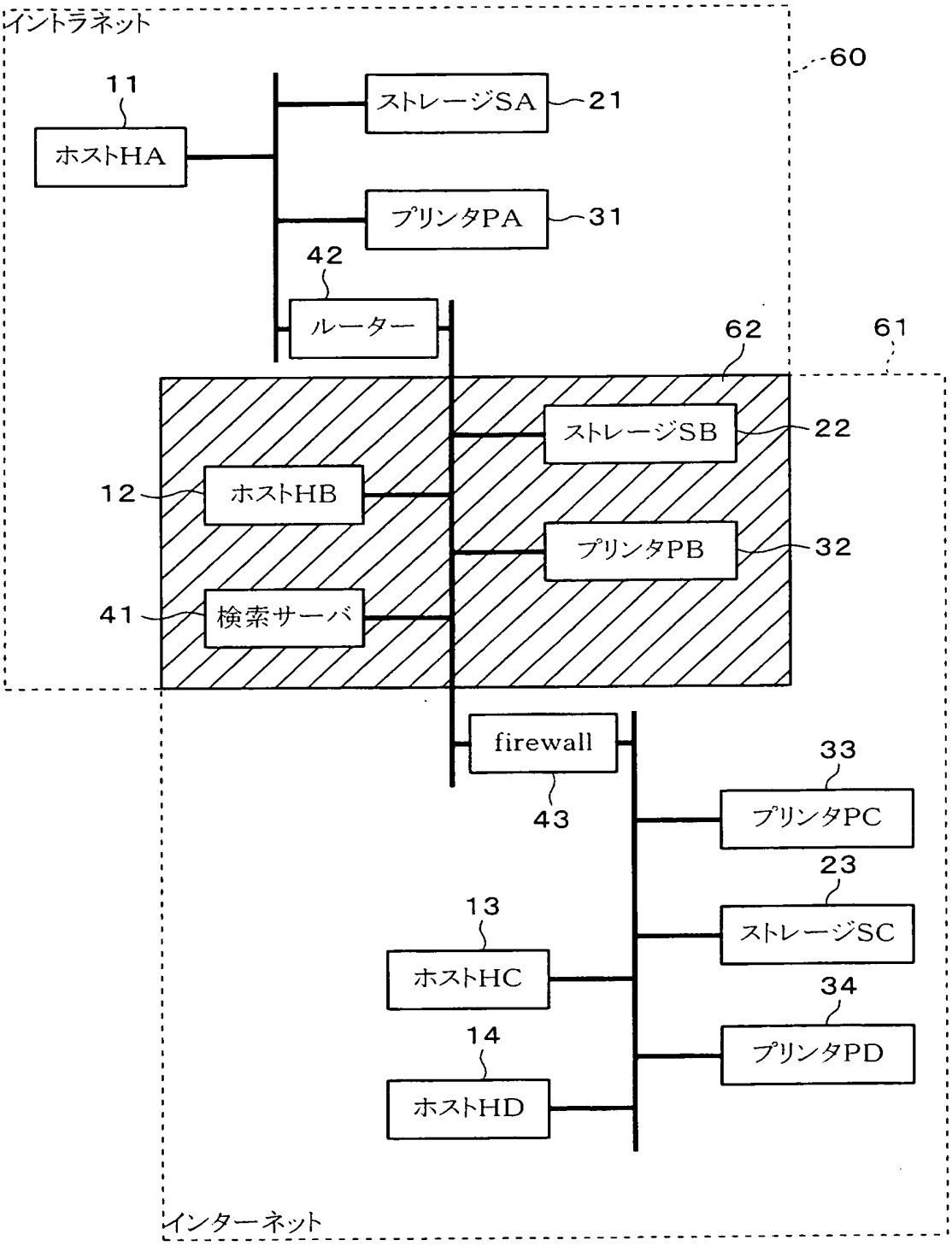
	ストレージ名	出力可能プリンタ	セキュリティ	料金
1	ストレージSA	プリンタPA	特高	200円
		プリンタPB	高	

OK　　戻る　　最初から　　プリンタの詳細

【図１１】


開始
検索ドライバ起動
S61
検索サーバに接続
S62
検索条件:ストレージを選択
S63
ストレージの検索条件を入力
S64
ストレージの検索結果を表示
S65
S66
選択
やり直す
ストレージ選択
S67
印刷可能？
NO
YES
印刷不可能なことを報知
S71
印刷データ取得
S68
S72
検索？
YES
印刷
S69
NO
印刷可能なプリンタを検索
S73
課金処理
S70
終了

【図１２】


イントラネット
60
11
ホストHA
ストレージSA
21
プリンタPA
31
42
ルーター
62
61
ストレージSB
22
12
ホストHB
プリンタPB
32
41
検索サーバ
firewall
43
33
プリンタPC
23
ストレージSC
13
ホストHC
34
プリンタPD
14
ホストHD
インターネット

【図１３】

（ａ）ホスト情報記憶部

ホスト名	接続可能 ストレージ	場所
ホストHA	イントラネット	××会社 本社
ホストHB	イントラネット インターネット	××会社 東京支社
ホストHC	インターネット ストレージSB	××インターネット
ホストHD	インターネット	△△インターネット

（ｂ）プリンタ情報記憶部

プリンタ名	接続可能 ストレージ	場所	機能
プリンタPA	イントラネット	××会社 本社	カラー、両面
プリンタPB	イントラネット インターネット	××会社 東京支社	両面、ステープル
プリンタPC	インターネット ストレージSB	○×コンビニ	カラー、両面、ステープル
プリンタPD	インターネット	△△コンビニ	カラー

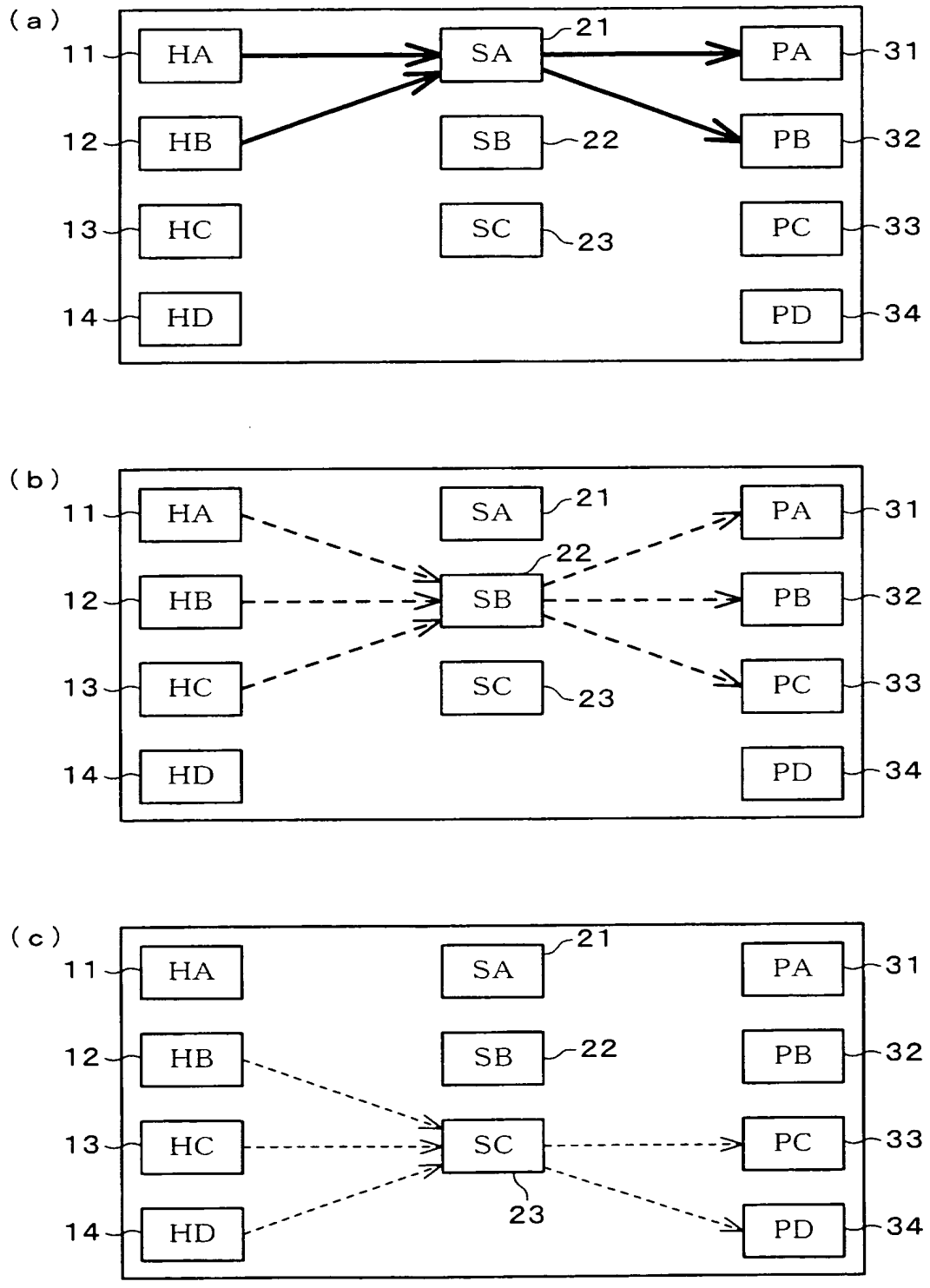
（ｃ）ストレージ情報記憶部

ストレージ名	接続可能 ホスト	接続(出力)可能 プリンタ	場所
ストレージSA	イントラネット	イントラネット	××会社 本社
ストレージSB	イントラネット ホストHC	イントラネット プリンタPC	××会社 東京支社
ストレージSC	インターネット	インターネット	××インターネット

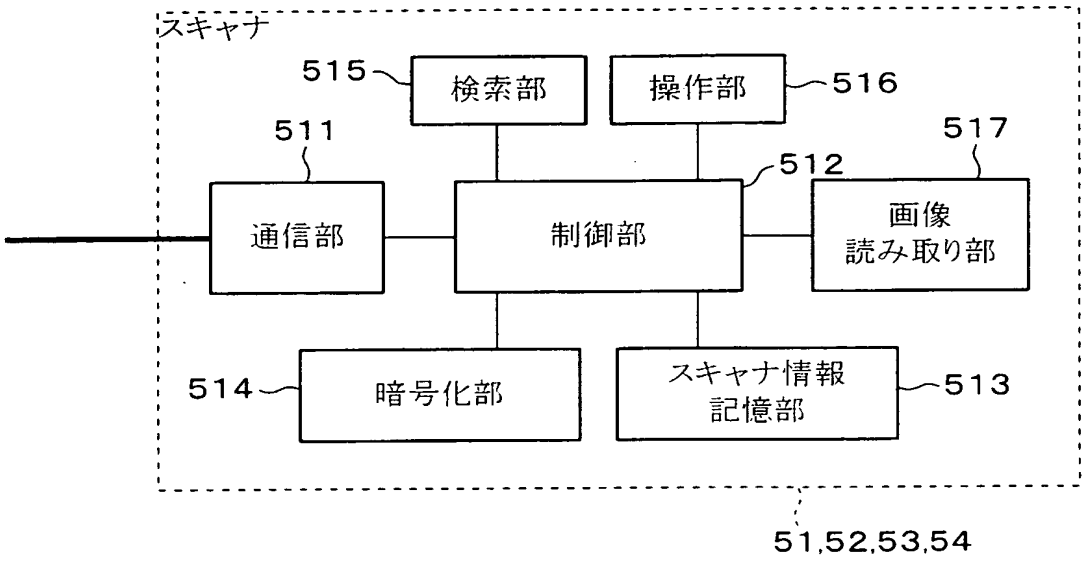
（ｄ）機器情報記憶部

ストレージ名	接続可能 ホスト	接続(出力)可能 プリンタ	セキュリティ レベル
ストレージSA	HA、HB	PA、PB	高
ストレージSB	HA、HB、HC	PA、PB、PC	中
ストレージSC	HB、HC、HD	PC、PD	低

【図１４】


(a)
11
HA
12
HB
13
HC
14
HD
SA
21
SB
22
SC
23
PA
31
PB
32
PC
33
PD
34
(b)
11
HA
12
HB
13
HC
14
HD
SA
21
SB
22
SC
23
PA
31
PB
32
PC
33
PD
34
(c)
11
HA
12
HB
13
HC
14
HD
SA
21
SB
22
SC
23
PA
31
PB
32
PC
33
PD
34

【図１５】


スキャナ
515
検索部
操作部
516
511
517
512
通信部
制御部
画像
読み取り部
514
暗号化部
スキャナ情報
記憶部
513
51,52,53,54

【図１６】

（ａ）ストレージ情報記憶部

ストレージ名	ストレージ使用料金	データ保護機能（レベル）	
ストレージ SA	200 円	暗号化プロトコル 2.0 のみ 暗号化保存	高（特高）
ストレージ SB	100 円	暗号化プロトコル 1.0 のみ	中
ストレージ SC	無料	－	低

（ｂ）スキャナ情報記憶部

スキャナ名	データ保護機能（レベル）		場所	スキャナ機能
スキャナ ScA	暗号化プロトコル 2.0 暗号化プロトコル 1.0 データの暗号化	特高	○○コンビニ 奈良店	カラー：2400dpi
スキャナ ScB	暗号化プロトコル 2.0 暗号化プロトコル 1.0	高	○○コンビニ 天理店	カラー：2400dpi
スキャナ ScC	暗号化プロトコル 1..0	中	○○コンビニ 郡山店	カラー：1200dpi
スキャナ ScD	－	低	○○コンビニ 高田店	モノクロ：600dpi

（ｃ）ホスト情報記憶部

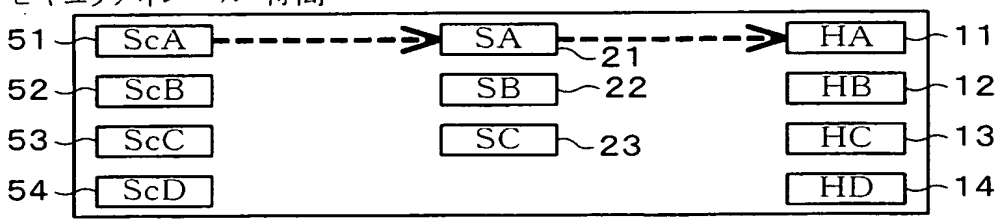
ホスト名	データ保護機能	データ暗号復号機能
ホスト HA	暗号化プロトコル 2.0 暗号化プロトコル 1.0	あり
ホスト HB	暗号化プロトコル 2.0 暗号化プロトコル 1.0	なし
ホスト HC	暗号化プロトコル 1.0	あり
ホスト HD	－	なし

（ｄ）機器情報記憶部

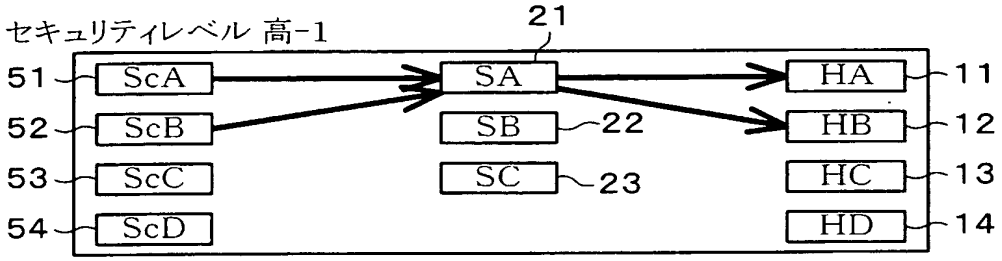
ルート	暗号化プロトコル	データ暗号化	セキュリティレベル
ScA→SA→HA	2.0	あり	特高
ScA、ScB→SA→HA、HB	2.0	なし	高
ScA→SB→HA、HC	1.0	あり	
ScA、ScB、ScC →SB →HA、HB、HC	1.0	なし	中
ScA→SC→HA、HC	なし	あり	
ScA、ScB、ScC、ScD →SC →HA、HB、HC、HA	なし	なし	低

【図１７】

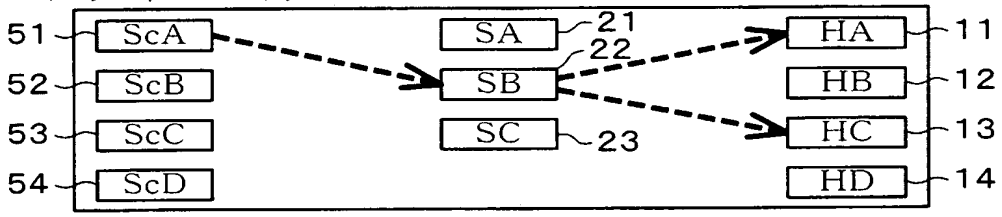
（ａ）セキュリティレベル 特高



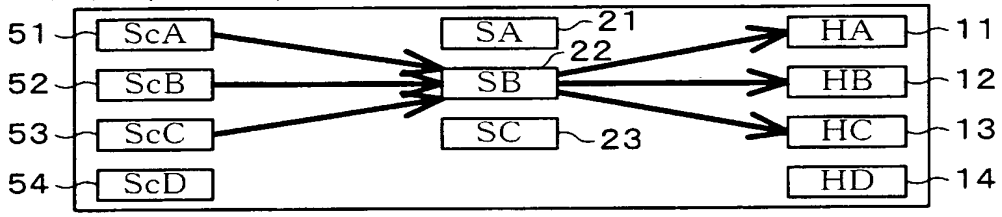
（ｂ）セキュリティレベル 高-1



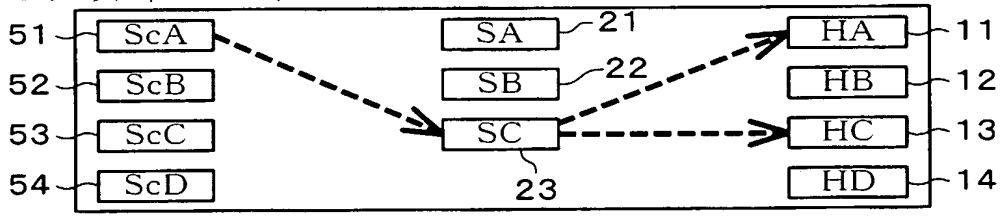
（ｃ）セキュリティレベル 高-2



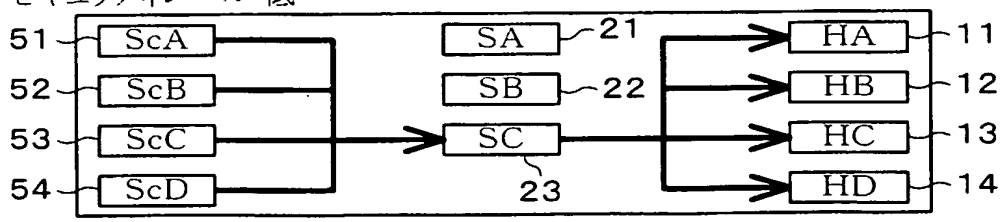
（ｄ）セキュリティレベル 中-1



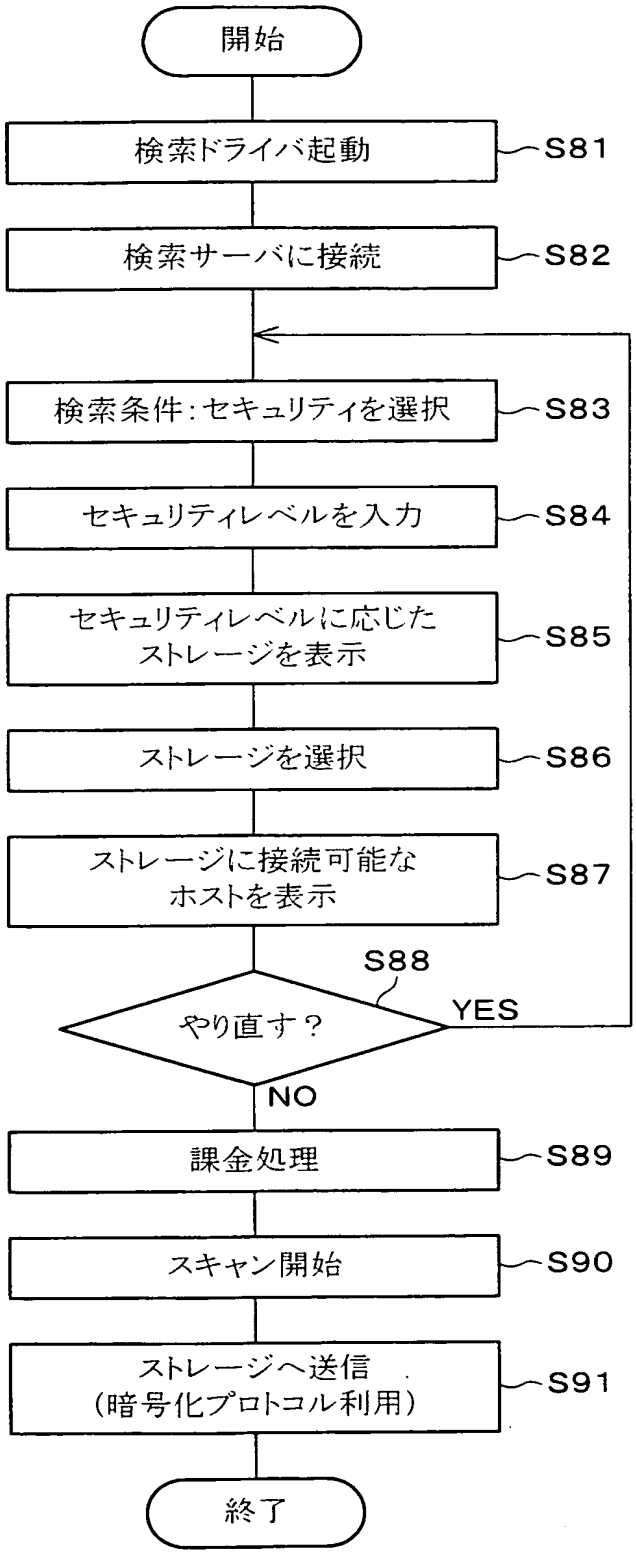
（ｅ）セキュリティレベル 中-2



（ｆ）セキュリティレベル 低



【図１８】


開始
検索ドライバ起動
S81
検索サーバに接続
S82
検索条件：セキュリティを選択
S83
セキュリティレベルを入力
S84
セキュリティレベルに応じた
ストレージを表示
S85
ストレージを選択
S86
ストレージに接続可能な
ホストを表示
S87
S88
やり直す？
YES
NO
課金処理
S89
スキャン開始
S90
ストレージへ送信
（暗号化プロトコル利用）
S91
終了

【書類名】　要約書

【要約】

【課題】

ネットワークを構成する電子機器間において送信されるデータの保護（セキュリティ）を考慮しつつ、ユーザが自由にセキュリティレベルに応じた送信ルートでデータの送信を行うことが可能な電子機器ネットワークシステムおよび電子機器ネットワークシステムによるデータ送信先検索方法を提供する。

【解決手段】

本発明の印刷システムは、複数のホストＰＣ１１～１４、複数のストレージ２１～２３および複数のプリンタ３１～３４を備え、それぞれがインターネットを介して接続されている。各ホストＰＣ１１～１４、各ストレージ２１～２３および各プリンタ３１～３４には、３種類のデータ保護機能が各機器ごとに付与されており、３段階のセキュリティレベルを有している。

【選択図】　図１

特願２００３－０２０９３７

出　願　人　履　歴　情　報

識別番号　　［０００００５０４９］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　　シャープ株式会社